LAHDEN AMMATTIKORKEAKOULU
Lahti University of Applied Sciences

KOULUTUSKONSERNIN SIIRTYMINEN IPV6-PROTOKOLLAAN

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikka
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2012
Aridani Paulin

Lahden ammattikorkeakoulu
Tietotekniikka

PAULIN, ARIDANI: Koulutuskonsernin siirtyminen IPV6-protokollaan

Tietoliikennetekniikan opinnäytetyö, 47 sivua

Kevät 2012

TIIVISTELMÄ

TCP/IP-protokolla otettiin käyttöön ARPANET-verkossa 1980-luvulla. TCP/IP-protokolla toimi edelleen siirryttäessä ARPANET-verkosta internetiin. TCP/IP- ja ipv4-protokolla suunniteltiin aikanaan hyvin ja ne toimivat hyvin. Internet kaupallistettiin 1990-luvulla, ja käyttäjämäärät ovat kasvaneet siitä lähtien. Internetin palvelut ja niitä käyttävien laitteiden määrä ovat kasvaneet viime vuosina räjähdysmäisesti. Uudet internetin palvelut ja ominaisuudet sekä käyttäjämäärän kasvu ovat asettaneet ip-protokollalle uusia vaatimuksia, joita ei voida rakentaa ipv4-protokollaan. Tämän takia kehitettiin uusi ipv6-protokolla, johon tehtiin suuria muutoksia, jotta ipv6-protokolla toimii mahdollisimman pitkään ja olisi mahdollisimman joustava.

Päijät-Hämeen koulutuskonsernin (myöhemmin PHKK) tietohallinto on alkanut kartoittaa ja suunnitella tietoverkkonsa päivittämisen ipv6-protokollaan. Tämä opinnäytetyö käsittelee ipv6-protokollaa, protokollan muutoksia ipv4-protokollaan ja eri siirtymätekniikoita. Tämän opinnäytetyön tiedoilla PHKK:n tietohallinto saa selville, kykynevätkö PHKK:n ohjelmistot ja palvelut käyttämään ipv6-protokollaa.

Testiympäristö rakennettiin virtuaalipalvelinalustalle. Virtuaalipalvelinalustalla pyöritettiin kahta eri palvelinta: Domain Controller -palvelinta sekä DFS-tiedostopalvelinta. Windows 7 Enterprise asennettiin asiakaskoneeksi virtuaalipalvelinalustalle. Testiympäristössä käytetään siirtymätekniikkana Dual stack -tekniikkaa PHKK:n vaatimuksesta.

Tämän opinnäytetyön tavoitteena oli tutkia, mitä muutoksia ja päivityksiä PHKK:n tietoverkko vaatisi, jotta tietoverkko voisi siirtyä käyttämään ipv6-protokollaa. Testiympäristön verkon rakentaminen pysähtyi operaattorin kohtaamiin ongelmiin, joten täydellistä testaamista ei voitu suorittaa. Tämän vuoksi kehitettiin testaussuunnitelma, jonka avulla voidaan testata ohjelmistojen ja palveluiden toimivuus ipv6-protokollalla. Siirtymisen aloittaminen ipv6-protokollaan vaatii aluksi paljon omien järjestelmien tutkimustyötä, mutta itse siirtyminen käytännössä ei tule olemaan vaikea.

Asiasanat: ipv6, siirtymätekniikat, Windows

Lahti University of Applied Sciences
Degree Programme in Telecommunications Technology

PAULIN, ARIDANI: Introduction of IPv6 at Educational Consortium

Bachelor's Thesis in telecommunications, 47 pages

Spring 2012

ABSTRACT

The TCP/IP protocol was taken to use in the ARPANET network in the 1980s. The TCP/IP protocol still worked when turning from the ARPANET network to the internet network. The TCP/IP protocol and ipv4 protocol were well designed and they worked well. The internet was commercialized in the 1990s and the number of users has increased since then. The services of the internet and the user devices have increasing exponentially in recent years. New services and features of the internet and increase number of users have set new requirements that cannot be accommonted into ipv4 protocol. That is why the new ipv6 protocol was developed with lots of changes so that the ipv6 protocol would work as long as possible and be as flexible as possible.

The IT administration of the Lahti Region Educational Consortium has begun to explore and design the data network upgrade to ipv6 protocol. This thesis deals with the ipv6 protocol and makes comparisons between the ipv6 protocol and the ipv4 protocol and different transition technologies. With the results of this thesis, the IT administration of the Lahti Region Educational Consortium will know, whether their software and service can use the ipv6 protocol.

The test environment was built on the virtual server platform. The Domain controller server and DFS server was run on the virtual server platform. Windows 7 Enterprise was installed as a client on the virtual server platform. The IT administration of the (Lahti Region Educational) Consortium required Dual stack technology as the transition mechanism in the test environment.

The goal of this thesis was to explore what changes and upgrades the network of the Lahti Region Educational Consortium needs to introduce the ipv6 protocol. Perfect testing could not be done because building the network of the test environment stopped when the teleoperator confronted problems. Therefore, a test plan was developed, which can be used to test the functionality of software and services with ipv6 protocol. Before begin to introduce ipv6 protocol, the explore process of the own systems takes lot of time but the transition process will not be difficult in practice.

Key words: ipv6, transition mechanisms, Windows

SISÄLLYS

LYHENNELUETTELO

Apache	Avoimeen lähdekoodiin perustuva HTTP-palvelinohjelma.
API	Application programming interface. Ohjelmointirajapinta, jonka avulla ohjelmat voivat keskustella keskenään.
ARPANET	Advanced Research Projects Agency. Internet:ä edeltävä tietoverkko.
CIDR	Classless Inter-Domain Routing. Mahdollistaa ipv4-osoitteiden jakamisen pienempiin aliverkkoihin.
DHCPv4	Verkkoprotokolla, joka jakaa ipv4-osoitteita niitä tarvitseville laitteille.
DHCPv6	Verkkoprotokolla, joka jakaa ipv6-osoitteita niitä tarvitseville laitteille.
DNS	Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset ip-osoitteiksi.
DNS64	Nimipalvelujärjestelmä, joka muuntaa verkkotunnukset ipv6-osoitteiksi.
IETF	Organisaatio, joka vastaa internetprotokollien standardoinnista.
IIS	Microsoftin kehittämä web-palvelinohjelmisto.
IP	Internet Protocol. TCP/IP-mallin internetkerroksen protokolla.
IP-osoite	Osoite, jota tietokoneet käyttävät liikennöidessään internetissä.

IPV4	Internet Protocol version 4 on nykyään käytössä oleva IP-protokollan versio.
IPV6	Internet Protocol version 6 on uusin IP-protokollan versio, joka tulee korvaamaan ipv4:n.
ISO	International Standards Organization. Kansainvälinen standardointijärjestö.
MAC-osoite	Verkkosovittimen osoite lähiverkoissa.
NAT	Network Address Translation. Osoitteenmuunnostekniikka, jolla säästetään julkisia ip-osoitteita.
NAT64	Osoitteenmuunnostekniikka, jossa ipv6-osoitteet piilotetaan julkiseen ipv4-osoitteeseen asioidessa ipv4-palvelimiin.
OSI-malli	Open Systems Interconnection. ISO:n luoma kerrosmalli, jota tietoliikennejärjestelmät käyttävät.
PAT	Porttimuunnostekniikka. Julkiseen ipv4-osoitteeseen lisätään porttinumero, jolloin yhdessä osoitteessa voi olla useampi yhteys.
RFC	Request for Comments. IETF:n julkaisemia internet-standardeja.
Tietosähke	IP-paketti. Viesti, joka siirretään IP-verkoissa.
TCP	Transmission Control Protocol. Tietoliikenneprotokolla, jolla luodaan yhteyksiä tietokoneiden välille.
WWW	World Wide Web. Hajautettu hypertekstijärjestelmä

1 JOHDANTO

Internetin perustamisen aikoihin kehitettiin IP-protokolla, joka on mahdollistanut internetin luomisen ja käytön. IP-protokollan ipv4-osoitteet ovat toimineet ja riittäneet hyvin näihin päiviin saakka. Internetin kasvanut käyttäjäkunta, päätelaitteiden määrä ja uudet vaatimukset sekä ominaisuudet vaativat uutta protokollaa, jotta internetin käyttö kehittyisi ja olisi sulavaa. Näiden asioiden vuoksi on kehitetty ipv4-protokollalle seuraaja, ipv6-protokolla. Ipv6-protokollan suurempi osoiteavaruus, kehyksen muokattavuus ja joustavampi toiminta pitäisi vain ottaa käyttöön.

Päijät-Hämeen koulutuskonserni (PHKK) on maakunnallinen koulutuksen järjestäjä 13:ssa eri jäsenkunnassa. PHKK järjestää, johtaa ja koordinoi jäsenkuntiensa puolesta ammattikorkeakoulutusta, lukio- ja ammatillista koulutusta, oppisopimuskoulutusta sekä kuntoutusta ja työhönvalmennusta. Päijät-Hämeen koulutuskonsernin tulosalueita ovat Koulutuskeskus Salpaus, Lahden ammattikorkeakoulu ja Tuoterengas. Päijät-Hämeen koulutuskonsernissa on vajaa 13 000 päätoimista opiskelijaa vuonna 2010. Henkilöstöä on reilu 1700. (Päijät-Hämeen koulutuskonserni 2012a).

Tietohallintopalvelut ylläpitää konsernin oppilaitoksille ja muille yksiköille erilaisia tietoliikennepalveluja. Tietohallintopalveluihin kuuluvat asiakaspalvelut, tietojärjestelmäpalvelut, tietotekniikkapalvelut ja tietohallinnon sisäiset palvelut. Tietohallintopalveluilla on paljon hallinnoitavia laitteita, palvelimia noin 130 kappaletta, verkon aktiivilaitteita noin 400 kappaletta ja käyttäjiä noin 20 000 kappaletta. (Päijät-Hämeen koulutuskonserni 2012b.)

Tämän opinnäytetyön tavoite on tutustua ipv6-protokollaan, tutkia ipv6-protokollan uusia ominaisuuksia, eri siirtymistekniikoita ja eroavaisuuksia ipv4-protokollaan. Ipv4-protokolla on ollut käytössä 1980-luvulta lähtien ja protokollan ominaisuudet alkavat olla riittämättömät nykyajan tiedonsiirtoon. Kehitystyön jälkeen syntyi uusi ipv6-protokolla, jonka ominaisuudet vastaavat paremmin nykyajan ja tulevaisuuden tarpeita.

Työn tilaaja on määritellyt käytettävän siirtymistekniikan, jota on tarkoitus kokeilla käytännössä rakentamalla testiympäristö. Testiympäristön rakentaminen

pysähtyi operaattorin toimintaan, joten työn lopuksi kehitetään testaussuunnitelma, jonka perusteella ipv6-protokollan toimintaa ja siirtymistekniikan toimivuutta kokeillaan sekä testataan eri ohjelmistojen ja palveluiden toiminta uudella protokollalla. Tämän opinnäytetyön avulla PHKK:n tietohallinto tulee saamaan tietoa ipv6-protokollaan siirtymisestä.

2 PERUSKÄSITTEET

2.1 Internet

2.1.1 Historia

Kun Neuvostoliitto laukaisi Sputnik I -satelliitin vuonna 1957, Yhdysvaltojen presidentti Dwight Eisenhower antoi ARPA:lle (Advanced Research Projects Agency) toimeksiannon kehittää ARPAnet:n, jotta Neuvostoliiton teknologinen etumatka asevarustelussa saataisiin kiinni (Livinginternet 2012). Yhdysvaltojen viranomaiset alkoivat 1950-luvun lopulla suunnitella kommunikointijärjestelmää, joka toimisi sotien ajan eikä lamaantuisi isoista iskuista. Järjestelmän täytyi olla hajautettu, eikä siinä saisi olla keskusvalvontaa, jotta kommunikointijärjestelmä toimisi, vaikka sitä vastaan hyökättäisiin. (Opasmedia 2012.)

Vuonna 1961 julkaistiin ehdotus tiedonvälityksen pakettiteoriasta ja vuonna 1964 RAND-yhdistys ehdotti, että kaikkien verkossa olevien koneiden tulisi olla samanarvoisia (Opasmedia 2012). Hajautetut tietokoneet ja tietokoneiden samanarvoisuus sekä itsenäisyys riittäisi pitämään tietoverkkoa pystyssä, joten kenenkään ei tarvitsisi ylläpitää verkkoa keskustietokoneella (Wikipedia 2012e). Vuonna 1967 ARPAnet-projekti alkoi, ja pari vuotta myöhemmin saatiin muodostettua ensimmäinen yhteys Kaliforniassa kahden tutkimuskeskuksen välillä (Livinginternet 2012; Opasmedia 2012).

1970-luvun loppuun mennessä ARPAnet:iin oli liittynyt monia tutkimuslaitoksia ja laboratorioita ympäri Yhdysvaltoja (Opasmedia 2012). Globaali internet sai alkupotkun vuonna 1980, kun ARPA alkoi muuntaa verkossa olevia laitteita TCP/IP-yhteensopiviksi (Comer 2002, 6). Vuonna 1981 ARPAnet jaettiin kahtia, joista ensimmäinen muuttui sotilasverkko MILNET:ksi ja toinen säilyi akateemisessa käytössä ARPAnet:nä. ARPAnet:ssä oli käytössä NCP-protokolla (Network Control Program), ja se korvattiin vuonna 1983 TCP/IP-protokollalla, josta tuli nopeasti verkon käytetyin protokolla maailmassa. (Livinginternet 2012.)

1990-luvulle tultaessa ARPAnet:ä alettiin kutsua internetiksi ja se kaupallistettiin operaattoreille. Internet alkoi leviämään yrityksille sen tarjoamien sähköposti- ja tiedonsiirtopalveluiden takia. (Wikipedia 2012e.) Internetin todellinen vallankumous alkoi vuonna 1991, kun julkaistiin hypertekstipohjainen sovellus Gopher ja samalla syntyi WWW (World Wide Web). Jatkoa oli luvassa vuonna 1992, kun julkaistiin WWW-selailua varten ensimmäinen graafinen käyttöliittymä Mosaic. (Kaario 2002, 15.) Internetin palveluiden määrä kasvoi paljon 1990-luvun puolen välin jälkeen, kun käyttöön tulivat videopuhelut, pikaviestit ja WWW-palveluineen (Wikipedia 2012f).

2.1.2 Nykyaika

Internetistä on tullut maailmanlaajuinen tietoverkko, jossa ei ole yhtä tietoverkkoa, vaan se on lukuisa määrä yhteenkytkettyjä tietoverkkoja palvelimineen. (Wikipedia 2012e.) Internetin kehitystä ja standardointia valvoo ja ohjaa moni organisaatio, jotka ovat koottuna taulukkoon 1. (Kaario 2002, 16 - 17.) Protokollien standardointityöhön osallistuvat verkkolaitteiden valmistajat, tietokonevalmistajat, sovellusten tekijät sekä palveluntarjoajat. Yhteisellä päätöksellä standardeista luodut RFC-dokumentit ovat internetissä kaikkien käytettävissä. (Comer 2002, 11.)

TAULUKKO 1. Internetin organisaatioita (Kaario 2002, 16)

Organisaatio	Tarkoitus
Internet Society (ISOC)	Internetin katto-organisaatio
Internet Architecture Board (IAB)	Internetin tekninen kehitys
Internet Engineering Task Force (IETF)	Pääasiassa standardointi
Internet Research Force (IRTF)	Tutkimustyö
Internet Assigned Numbers Authory (IANA)	Numerointi ja nimeäminen
Internet Corporation for Assigned Names and	IANA:n seuraaja

Numbers (ICANN)	
World Wide Web Consortium (W3C)	WWW-organisaatio

Tiedonsiirtoverkkoja varten on pitänyt kehittää useita tiedonsiirtoprotokollia, vaikka niitä oli olemassa jo ennen internetiä. Uusia protokollia on pitänyt luoda ja kehittää, koska nykyistä tiedonsiirtojärjestelmää ei voitu luoda olemassa olevilla protokollilla. Sen vuoksi TCP/IP-protokollaperhettä ei keksitty vanhojen syrjäyttämisen toivossa, vaan luomaan uusia, yhteensopivia protokollia. (Comer 2002, 12.)

Internetin nopeaa kasvua ei osattu vielä hahmottaa 1980-luvulle tultaessa ja vuosikymmen puolivälissä törmättiin ensimmäiseen suureen ongelmaan. Kaikkien internetissä olevien tietokoneiden nimet ja osoitteet olivat yhdessä tiedostossa, jota kopioitiin kaikkiin internetin toimipaikkoihin. Kasvaneen käytön myötä tiedoston ylläpitäminen ei olisi onnistunut ja tiedoston kopioiminen jokaiseen toimipaikkaan olisi kuormittanut verkkoa liikaa. Siitä syystä kehitettiin DNS (Domain Name Server, nimipalvelimet) -palvelimet, jotka vastaavat verkossa tapahtuviin nimikyselyihin. DNS-palvelimet eivät sisällä kaikkia tietoja, vaan ne kyselevät toisiltaan tietoa ja vaihtavat tietoa keskenään käyttäen TCP/IP-protokollaa. (Comer 2002, 8.) Toinen internetin ongelma on tällä hetkellä ip-osoitteiden määrä, joka on loppumaisillaan.

2.2 OSI-malli

Tietoliikennetekniikassa monimutkaiset kokonaisuudet tehdään paremmin hallittaviksi ajattelemalla tehtävät asiat eri kerroksina. Verkko saattaa koostua useista erilaista järjestelmistä, jolloin kerrosajattelu auttaa järjestelmiä toimimaan oikein, kun tietyllä kerroksella suoritetaan tietyt toiminnot protokollien avulla. (Kaario 2002, 18.) Jokaisessa laitteessa ja järjestelmässä verkon kautta tuleva ja lähtevä data kiertää tietyn protokollapinon läpi, jotta dataa ymmärretään ja siirretään oikein.

Tietoliikenteessä on kaksi tärkeää protokollamallia, joihin törmäämiseltä ei voi välttyä. Ensimmäinen niistä on OSI-viitemalli (Open Systems Interconnection), joka on ISO:n (International Standards Organization) luoma malli. OSI-malli tarjoaa laitevalmistajille ja verkkojen käyttäjille ympäristön, jossa kaikki järjestelmät ymmärtävät toisiaan, eikä lukuisia, erilaisia verkkoja enää tarvita. OSI-malli ei ole saavuttanut ISO:n sille asettamia tavoitteita. Kuitenkin, OSI-malli loi kerrosajattelun, joka on nykyään lähes kaiken tietoliikenteeksi kutsuttavan perustana. (Kaario 2002, 18.)

Sovelluskerros	Application layer
Esitystapakerros	Presentation layer
Istuntokerros	Session layer
Kuljetuskerros	Transport layer
Verkkokerros	Network layer
Siirtokerros	Link layer
Fyysinen kerros	Physical layer

KUVIO 1. OSI-mallin kerrokset suomeksi ja englanniksi (Kaario 2002, 18)

Kuviossa 1 on kuvattu OSI-mallin seitsemän kerrosta. Jokaisella kerroksella on omia protokollia yksi tai useampi, jotka hoitavat datan siirron kannalta tärkeitä tehtäviä. Kolmea ylintä kerrosta kutsutaan yhteisellä nimellä ylemmät kerrokset ja neljää alinta kutsutaan nimellä alemmat kerrokset.

Fyysinen kerros huolehtii bittivirran siirtymisestä fyysisesti siirtomediassa. Fyysinen kerros vastaa muun muuassa siirtotien sähköisistä ominaisuuksista ja signaalien jännitetasoista. Fyysinen kerros poikkeaa muista kerroksista ottamalla kantaa fysikaalisiin ilmiöihin, kun muut kerrokset ovat lähinnä ohjelmistollisia. (Kaario 2002, 19.)

Fyysisellä kerroksella on lukuisia tärkeitä parametrejä ja tehtäviä, kuten siirtovirhesuhde, siirtonopeus ja siirtoviive sekä vastuu datansiirron synkronoinnista. Fyysinen kerros hoitaa datan moduloinnin tai pakkaamisen ennen siirtotielle lähettämistä. Fyysisellä kerroksella voidaan lähettää bittejä rinnakkain tai sarjassa. (Kaario 2002, 19.)

Siirtokerros vastaa bittivirran luotettavasta siirtymisestä, tutkii signaalin oikeellisuuden siirtovirheiden varalta ja lähettää data määrämuotoisissa paketeissa. Siirtokerros ei ota kantaa datan oikeellisuuteen, vaan tarkistaa siirrettyjen bittien oikeellisuuden. Siirtokerroksen tehtävänä on tarjota verkkokerrokselle datansiirtoyhteys kahden keskustelevan verkkolaitteen välille. Siirtokerros voi käyttää yhtä tai useampaa fyysistä yhteyttä kahden verkkolaitteen välillä, jotta yhteyden laatuvaatimukset täyttyvät. Näkyvin osa siirtokerrosta on sen MAC-kerros. MAC-kerros takaa siirtokerroksen reilun käytettävyyden eri käyttäjien kesken. MAC-kerroksen tunnetuin protokolla on CSMA/CD, jota käytetään Ethernet-lähiverkoissa. (Kaario 2002, 20.) MAC-kerroksella sijaitsee verkkokortin valmistajan kirjoittama 48 bittiä pitkä MAC-osoite, jota käytetään Ethernet-lähiverkkojen osoitteina (Wikipedia 2012a).

Verkkokerroksen ehdottomasti tärkein tehtävä on datapakettien reitittäminen. Verkkokerroksella voi olla palveluina esimerkiksi vuonvalvontaa ja laatuvaatimusten tarkkailua. (Kaario 2002, 20.) Reitittimet toimivat verkkokerroksella käyttäen ip-osoitteita ja jokaisella verkkoon kytketyllä laitteella tulee olla ip-osoite, jos laite haluaa asioida reitittimen läpi ulkomaailmaan. Verkkokerroksen näkyvin osa on ip-osoite. (Wikipedia 2012a.)

Kuljetuskerros muodostaa suoran yhteyden liikennöivien järjestelmien välille eli datan kuljettamisesta lähettäjältä vastaanottajalle. Kuljetuskerroksen protokollien tehtäviin kuuluu tarvittaessa huolehtia pakettien oikeasta vastaanottojärjestyksestä ja uudelleenlähetyksistä, mikäli paketteja on kadonnut siirron aikana. Kuljetuskerros on korkeimpana alimpien kerroksien ryhmässä ja kuljetuskerros toimii linkkinä ylimmille kerroksille. (Kaario 2002, 21.)

Istuntokerros on ensimmäinen ylemmistä kerroksista, joka ei varsinaisesti ole tekemisissä tietoliikenteen kanssa. Istuntokerros huolehtii yhteyksien

muodostamisesta ja purkamisesta liikennöivien järjestelmien välillä. (Kaario 2002, 21.) Istuntokerros sallii datan lataamisen useasta eri bittivirrasta tai eri lähteistä, jotka voidaan yhdistää tai synkronoida, esimerkiksi videoneuvottelu (Wikipedia 2012b).

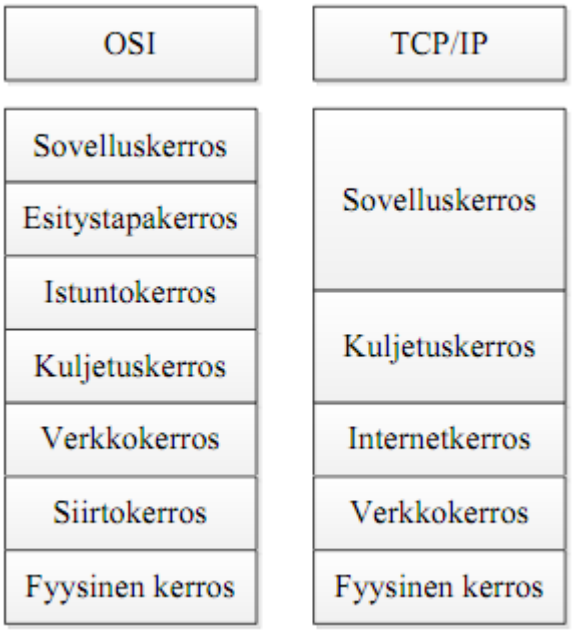
Esitystapakerros huolehtii nimensä mukaan siirron aikana käytettävästä esitystavasta (Kaario 2002, 21). Verkkoa käyttävät sovellukset käyttävät esitystapakerroksen sisältämiä toimintoja. Esitystapakerroksen toimintoja ovat esimerkiksi tekstin tai kuvan muuttaminen digitaaliseksi bittivirraksi. (Comer 2002, 183.)

Sovelluskerros on ylin OSI-mallin protokollakerroksista, eikä sen tarvitse tarjota palveluita ylemmälle kerrokselle, vaan se toimii lopullisena rajapintana sovelluksien ja tietoliikenneyhteyksien välillä. Sovelluskerros määrittelee verkkoa käyttäville sovelluksille yhtenäisen kommunikointirajapinnan, kuten sähköposti, tiedonsiirto ja hakemistopalvelut, jolloin näiden protokollia olisi esimerkiksi SMTP sähköpostille. (Kaario 2002, 21.)

2.3 TCP/IP -malli

TCP/IP -protokolla on toinen, tärkeä kerrosmalli, joka ei ole standardikomitean laatima, vaan TCP/IP-protokolla rakentui tutkimuksesta (Comer 2002, 183). TCP/IP-verkoilla yhdistetään joustavasti toisiinsa eri käyttötarkoituksiin suunniteltuja laitteita ja käyttöjärjestelmiä. TCP/IP:tä käytetään tavallisissa lähiverkoissa, langattomissa verkoissa sekä automaatioverkoissa. TCP/IP:tä voidaan käyttää missä tahansa, mihin on mahdollista toteuttaa TCP/IP -protokollaohjelmisto. (Kaario 2002, 14.)

TCP/IP -protokollaperheen nimi muodostuu kahdesta tärkeästä protokollasta: Internet Protocol (IP) ja Transmission Control Protocol (TCP). IP-protokolla toimii TCP/IP-mallin verkkokerroksella ja TCP-protokolla toimii kuljetuskerroksella. TCP/IP -protokollaan kuuluu lukuisia muita protokollia, kuten epäluotettava kuljetuskerroksen protokolla User Datagram Protocol (UDP), verkonhallintaprotokolla Simple Nerwork Management Protocol (SNMP) ja reititysprotokolla Open Shortest Path First (OSPF). (Kaario 2002, 15.)



KUVIO 2. OSI-malli ja TCP/IP -malli (Comer 2002, 184, Wikipedia 2012d)

Kuviossa 2 on kuvattu TCP/IP -mallin kerrosrakennetta ja verrattu sitä OSI-mallin kerrosrakenteeseen. Alinpana on fyysinen kerros, joka käsittää laitteistoa, jolla luodaan fyysinen yhteys verkkoon. Riippuen eri lähteistä, TCP/IP-mallissa on neljä tai viisi kerrosta, joissa OSI-mallin fyysinen kerros on mukana tai se on jätetty pois (Wikipedia 2012d).

Verkkokerros on TCP/IP-mallin alin kerros, joka vastaanottaa verkosta IP-paketit ja siirtää paketit oikeaan verkkoon (Comer 2002, 185). TCP/IP-malli ei määritä kovinkaan tarkkaan, mitä internetkerroksen alla tapahtuu. TCP/IP-malli olettaa, että IP:n alla on jokin protokolla, joka osaa välittää IP-paketit. IP-protokolla ei ota kantaa minkälaista fyysistä mediaa käytetään pakettien siirtämiseen, joten fyysisenä mediana voi olla esimerkiksi Ethernet, ADSL tai 3G-yhteys. (Wikipedia 2012c.)

Internetkerros hoitaa tiedonsiirron vastaanottamalla ylemmältä kerrokselta paketin lähetyspyynnön ja vastaanottajan ip-osoitteen. Internetkerros muokkaa pakettia lisäämällä sinne IP-osoitteet, otsikkotiedot ja lopuksi internetkerroksen protokollat tutkivat, täytyykö paketti lähettää reitittimelle vai paikalliseen verkkoon. Internetkerros vastaanottaa tulevat paketit, tarkistaa tietojen oikeellisuuden ja

tutkii reititysalgoritmien avulla, lähetetäänkö paketti edelleen verkkoon vai ylemmälle protokollalle. Paikalliseen lähiverkkoon pakettia lähetettäessä internetkerros poistaa paketin otsikon ja valitsee protokollan, joka kuljettaa paketin paikallisessa verkossa. (Comer 2002, 185.)

Kuljetuskerros hoitaa tiedon siirron kahden sovelluksen välillä, jota kutsutaan päästä-päähän (end-to-end) -siirroksi. Kuljetuskerros osaa säädellä tietovirtaa ja tarjoaa luotettavan tiedonsiirron tarkistamalla tietojen virheettömyyden ja järjestyksen. Tietojen oikean järjestyksen varmistamiseksi protokollaohjelmisto tarvitsee vastaanottajan kuittauksen saamistaan paketeista ja pakettien kadotessa lähettäjä lähettää ne uudelleen. Kuljetuskerros lisää tietovirtaan vastaanottajan osoitteen, tekee tietovirrasta pieniä paketteja ja siirtää paketit verkkokerrokseen. (Comer 2002, 184.)

Sovelluskerroksessa kautta käyttäjän käynnistämät sovellukset käyttävät TCP/IP-verkon palveluita. Sovellukset valitsevat itselleen sopivan siirtotavan kuljetuskerroksesta sovelluskerroksen kautta ja lähettävät datan kuljetuskerrokselle. (Comer 2002, 184.) TCP/IP -mallissa halutaan sovellusten hoitavan enemmän tehtäviä, kuten istuntojen muodostamisen ja purkamisen, jotka kuuluivat OSI-mallissa istunto- ja esitystapakerroksille. (Wikipedia 2012c.)

2.4 Internet protokolla versio 4

2.4.1 Osoitteet

Internet protocol (IP) on TCP/IP-mallin tärkein protokolla. IP:n avulla voidaan siirtää dataa melkein millä vain protokollalla ja IP:n yläpuolisella kuljetuskerroksella voidaan käyttää erilaisia kuljetusprotokollia. IP on yhteinen protokolla koko verkolle, ja kaikki verkon käyttäjät joutuvat käyttämään IP-kerroksen palveluita. (Kaario 2002, 46.)

Internet protokollaan kuuluvat ip-osoitteet. Erilliset ip-osoitteet on aikoinaan otettu käyttöön, koska on haluttu eritellä eri verkkoihin kuuluvat tietokoneet. MAC-osoitetta käytetään lähiverkon tiedonsiirrossa, mutta maailmanlaajuiseen

käyttöön MAC-osoite ei sovellu, koska sitä ei voida luokitella kuuluvaksi tietyn reitittimen alaisuuteen. Sen takia kehitettiin ip-osoitteet ja data reititetään ip-osoitteen perusteella oikeaan lähiverkkoon, jossa käytetään MAC-osoitteita. Oikeaan elämään sijoitettuna MAC-osoite vastaa henkilön katuosoitetta ja ip-osoite vastaa postiosoitetta. Postinlajittelukeskus katsoo postinumeron perusteella, mille alueelle kirje kuuluu toimittaa, ja kirje laitetaan oikeaan lajittelulaatikkoon. Postinjakaja katsoo kirjeestä, mihin osoitteeseen kirje täytyy toimittaa, ja toimittaa kirjeen perille. Tietoliikennetekniikassa reititin katsoo ip-osoitteen verkko-osasta, minne aliverkkoon datapaketti lähetetään ja aliverkon reunalla toinen reititin katsoo, mihin MAC-osoitteeseen datapaketti lähetetään. Ip-osoitteita annetaan yksilöllisesti tietokoneille, jotta tietokoneet voivat kommunikoida internetissä. (Kaario 2002, 53.)

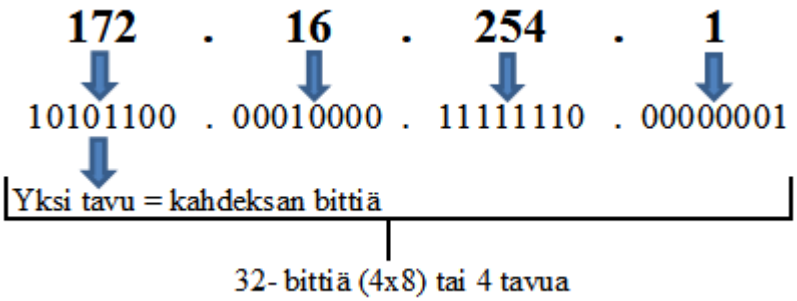
Internet protokolla version 4 osoitteet ovat 32-bittisiä osoitteita. Ip-osoitteita on julkisia ja yksityisiä, niin sanottuja villejä osoitteita. Yksityisiä osoitteita ei saa reitittää julkiseen verkkoon. Aluksi ip-osoitteiden käyttö aloitettiin A-luokan osoitteista, koska ajateltiin, että muutama suuri verkko riittäisi. Verkkojen määrän kasvaessa otettiin B-luokka käyttöön keskisuurille verkoille ja C-luokka otettiin käyttöön pienille verkoille. Taulukossa kaksi on esitelty RFC 1918 -dokumentin yksityiset osoitteet ja teoriassa käytettävissä olevien työasemaosoitteiden määrä. (Kaario 2002, 54, 57.)

TAULUKKO 2. Yksityiset ip-osoitteet (Kaario 2002, 54; Wikipedia 2012i)

Verkkoluokka	Varatut osoitteet	Maski	Osoitteiden määrä
A-luokka	10.0.0.0 – 10.255.255.255	255.0.0.0	16777216
B-luokka	172.16.0.0 – 172.31.255.255	255.240.0.0	1048576
C-luokka	192.168.0.0 – 192.168.255.255	255.255.0.0	65536
D-luokka	224.0.0.0 – 239.255.255.255	-	
E-luokka	240.0.0.0-255.255.255.255	-	

Teoriassa tässä versiossa osoitteita on 2^{32} eli 4 294 967 296 kappaletta, joista käyttökelpoisia ip-osoitteita on arviolta 3,2 - 3,3 miljardia kappaletta. Ipv4:n osoiteavaruudesta on varattu pienempiä osoiteavaruuksia erilaisiin käyttötarkoituksiin. Ensimmäinen ryhmä ovat 127-alkuiset ip-osoitteet. Niitä kutsutaan loopback-osoitteiksi eli takaisinkytketyiksi osoitteiksi. Ne on tarkoitettu tietokoneen tai reitittimen sisäiseen käyttöön. Toisen ryhmän muodostavat D-luokan osoitteet, jotka ovat väliltä 224.0.0.0 – 239.255.255.255. D-luokka on varattu ryhmälähetyksiin (broadcast), eikä niitä voi käyttää yksittäisille laitteille. Kolmannen ryhmän muodostavat E-luokan osoitteet väliltä 240.0.0.0 – 255.255.255.254. E-luokan osoitteet on varattu kokeilukäyttöön. E-luokkaan kuuluu myös yksittäinen ip-osoite 255.255.255.255, jota käytetään lähettämään broadcast-viesti kaikille saman aliverkon laitteille. (Kaario 2002, 57 - 58; Desmeules 2007, 6; Cisco 2011b.) Lisäksi on lukuisia muita pieniä avaruuksia 24-bittisellä maskilla, joille on omat erikoiskäyttökohteensa (Wikipedia 2012j).

Ip-osoitteet muodostuvat neljästä oktetistä eli tavusta. Yhdessä tavussa on kahdeksan bittiä. Ipv4-osoitteen pituus on 32 bittiä. Kuviossa kolme on esitetty ip-osoite 172.16.254.1 desimaalimuodossa ja binäärimuodossa.



KUVIO 3. Ipv4-osoite desimaalimuodossa (Wikipedia 2012i)

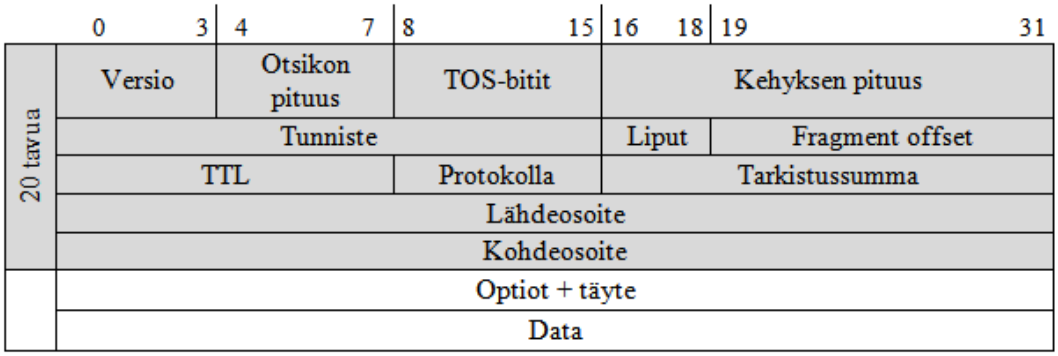
Ip-osoitteet olivat aluksi luokallisia osoitteita, mutta osoitteiden luokallisuus hukkasi paljon osoitteita ja ajanmittaan osoitteet uhkasivat loppua. Tämän takia siirryttiin luokattomiin ip-osoitteisiin, CIDR (Classless Inter-Domain Routing), jolloin ip-osoitteen maski luokittelee ip-osoitteet aliverkkoihin. (Comer 2002, 64.)

CIDR otettiin käyttöön vuonna 1993 ja se kehitettiin säästämään ip-osoitteita poistamalla ip-osoitteiden luokituksen (Wikipedia 2012g). CIDR:n osoitesäästö perustuu aliverkkomaskin käyttämiseen, jolla voidaan ottaa käyttöön vain tarvittava määrä ip-osoitteita. CIDR:n käyttöönotto helpotti myös reitittimien työtä, kun CIDR pienensi reitittimien reititystauluja. Ennen reitittimessa oli yksi rivi jokaista mainostamaansa aliverkkoa kohti. Nyt saman verkko-osan aliverkot pystytään mainostamaan yhdellä aliverkon mainoksella. Esimerkiksi aliverkko 20.1.4.0 /24 voitiin mainostaa 20.1.0.0/16-verkon kanssa, koska niiden verkko-osa, 20.1, on yhteinen. (Kaario 2002, 86.)

Toinen tekniikka, jolla pyritään tehostamaan ip-osoitteiden käyttöä, on NAT (Network Address Translation). NAT-tekniikka kehitettiin, koska huomattiin, ettei kaikille maailman tietokoneille riitä ip-osoitteita. (Wikipedia 2012h.) NAT-tekniikoita on neljä erilaista: staattinen, dynaaminen, overloading ja overlapping. Staattisessa NAT-tekniikassa yksi yksityinen ip-osoite saa yhden julkisen ip-osoitteen ja käyttää aina samaa julkista ip-osoitetta. Dynaamisessa NAT-tekniikassa yksityinen ip-osoite saa sattumanvaraisesti yhden julkisen ip-osoitteen esimerkiksi yrityksen käytössä olevista julkisista ip-osoitteista. Staattinen ja dynaaminen NAT ei säästä julkisia ip-osoitteita. Sen vuoksi on kehitetty NAT overloading-toiminnolla, jota kutsutaan myös PAT:ksi (Port Address Translation). Overloading naamioi yksityiset ip-osoitteet yhdeksi julkiseksi ip-osoitteeksi, johon lisätään porttinumero jokaiselle yksityiselle ip-osoitteelle. Overlapping NAT:a käytetään silloin, kun sisäverkossa käytetään julkisia ip-osoitteita, jotka ovat mahdollisesti muuallakin käytössä. Tämän takia reititin muuttaa sisäverkon ip-osoitteet erilaisiksi liikennöidessä ulkoverkkoon, jolloin vältytään ip-osoitteiden ristiriidalta. NAT-muunnoksen tekee reititin tai palomuuri sisä- ja ulkoverkon välisellä rajalla. (Comer 2002, 394; Cisco 2011b.)

2.4.2 Kehysrakenne

Kuviosta neljä nähdään ipv4:n kehys. Kehys on 32 bittiä pitkä, ja siinä on 20 tavua (harmaalla kuviossa neljä). Kuvion neljä optiot + täyte ja data ovat edellämainitun 20:n tavun ulkopuolella. (Kaario 2002, 46.) Kuviossa neljä esitetyillä kentillä on omat käyttötarkoituksensa, joita käydään läpi.



KUVIO 4. IPv4 kehys

Versio-kenttä on neljä bittiä pitkä, ja siinä kerrotaan kehyksen versio. Tällä varmistutaan, että kaikki laitteet, jotka käyttävät kyseistä kehystä, tulkitsevat kehyksen oikein. Otsikon pituus -kenttä on myös neljä bittiä pitkä, ja se kertoo, kuinka monta 32 bittiä pitkää sanaa, eli oktettia, otsikossa on. TOS-kenttä on kahdeksan bittiä pitkä, jossa bitit kolme, neljä, viisi ja kuusi kertovat kehyksen laatuvaatimuksen. TOS-kentässä voidaan määrittää kehyksen tärkeys, viive, siirtoteho, luotettavuus ja hinta, mutta vain yksi vaatimus saa olla kerralla asetettuna. 1990-luvun loppupuolella IETF määritteli TOS-kentän uudelleen, sijoittaen sinne DSCP:n (differentiated services codepoint) ja ottaen käyttöön DiffServ-käsitteen (differentiated services). (RFC 1349 1992; RFC 2450 1998; Comer 2002, 98 - 99; Kaario 2002, 46 - 47.)

Kehyksen pituus kertoo kehyksen kokonaispituuden 16:lla bitillä, jolloin yhden ip-kehyksen kokonaispituus voi olla 2^{16} eli 65535 oktettia. Tunniste-kenttää käytetään identifioimaan paketit, jotka on pilkottu samasta ylemmän protokollakerroksen viestistä. Ilman tunniste-kenttää vastaanottaja ei tietäisi, mitkä paketit ovat samasta viestistä. Lippujen kolme bittiä kertovat pakettien pilkkomisesta. M-bitti kertoo, että kyseisen paketin jälkeen tulee vielä muita paketteja, jotka ovat saman viestin osia. D-bitti kertoo, että kyseistä ip-pakettia ei saa pilkkoa enään pienempiin osiin. (Kaario 2002, 48 - 49.)

Fragment Offset -kenttä kertoo vastaanottopäässä, missä järjestyksessä pilkottu kehys täytyy koota. TTL eli Time to live -kenttä kertoo, miten kauan paketilla on vielä elinaikaa, eli kuinka monen reitittimen läpi paketti voi kulkea ennen kuin se

tuhotaan. Aluksi paketit saavat TTL-arvokseen 255. Paketin elinaika on määrätty hyppyinä, eli aina kun paketti reitittimeltä jatkamaan eteenpäin, TTL-arvosta vähennetään yksi. Näin verkkoon ei jää turhia paketteja harhailemaan. Kun paketin elinaika loppuu eikä paketti ole saavuttanut määränpäätä, paketin hylännyt reititin lähettää tiedon hylkäyksestä hylätyn paketin lähdeosoitteeseen. Protokollan tunniste -kenttä kertoo, miltä protokollalta data siirtyi ip-kerroksen lähetettäväksi. (Kaario 2002, 49 - 50.)

Tarkistussumma-kenttää käytetään kehyksen tarkistamiseen. Tarkistussumma saadaan, kun ip-protokollaa käyttävät ylemmät protokollat laskevat sen omilla menetelmillään. Lähde- ja kohdeosoitteet ovat 32-bittisiä ipv4-osoitteita. Optiot-kenttä on varattu erilaisille toiminnoille, joista suurinta osaa ei käytetä. Täytettä käytetään, jos paketin koko ei lopu 32 bitin monikertaan. Tarvittaessa pakettiin lisätään nollia loppuun. (Kaario 2002, 49 - 50.)

3 IPV6

3.1 Yleistä ipv6-protokollasta

1980-luvun alussa käyttöönotetun ipv4:n kaikki mahdolliset julkiset osoitteet ovat loppumassa. Osoitteiden loppumista vauhdittavat langattomien päätelaitteiden määrällisesti räjähdysmäinen kasvu, kolmannen maailman vaurastuminen sekä uudet sovellukset ja käyttökohteet. Ipv4 on hoitanut työnsä hyvin, ja on aika siirtyä ipv6:een.

Swinburnen teknillisen yliopiston tutkijat ennustavat, että Euroopassa ip-osoitteita hallinnoivan RIPE:n ipv4-osoitteet ovat loppumassa heinäkuun 22. päivä vuonna 2012. Aasian maanosaorganisaatio Apnicin ip-osoitteet ovat arvioiden mukaan loppumassa huhtikuussa samana vuonna. Tämän jälkeen internetin käyttö ipv4-protokollalla hieman vaikeutuu. Ratkaisu osoitteiden loppumiselle on ipv6-protokolla, jonka osoitemäärä ei pitäisi loppua koskaan. (Rinta 2012.)

Ipv4:n pitkä tie lähes muuttumattomana 1980-luvun alusta tähän päivään on tietotekniikan alalla iso asia. Ipv4 suunniteltiin aikoinaan hyvin ja se on toiminut, vaikka ipv4:sta käyttävät laitteet ja sovellukset sekä niiden määrä ovat kehittyneet huimasti. Nykypäivän tiedonsiirron tarpeisiin ipv4 alkaa kuitenkin olemaan jo hieman vanhanaikainen. VOIP-puheluiden ja muiden reaaliaikaisten palveluiden yleistyminen, tietoturvan tärkeys sekä osoiteavaruuden pienuus ovat pakottaneet kehittämään ipv6:n ja kohta siirtymään ipv6:een. (Comer 2002, 600 - 601.)

Nykyisin jotkin verkkopalvelut tarjoavat palveluita ipv6-protokollalla. Esimerkiksi Facebook tiedotti kesäkuussa 2010 ottavansa käyttöön ipv6:n käyttämällä reitittimiensä dual stack -tukea (Marsan 2010). Google oli Facebook:a nopeampi ja aloitti ipv6-tuen käyttöönoton jo maaliskuussa 2008. Syyskuusta 2008 alkaen käyttäjät ovat voineet käyttää Googlen hakua ipv6-yhteyksillä (Google 2011). Aluksi tuki otettiin käyttöön vain hakupalvelussa, mutta tuki laajennetaan kaikkiin Googlen virtuaalisiin palveluihin World ipv6 -päivänä kesällä 2012 (Kline 2012).

3.2 Historia ja kehitys

IETF:llä kesti vuosia muotoilla uusi versio ip:stä. Avoimen standardin vuoksi IETF pyysi koko käyttäjäkuntaa kehittämisprosessiin. Kehittämisprosessissa olivat mukana muun muuassa tietokone- ja laitevalmistajat, järjestelmähallitsijat, ohjelmoijat, puhelinyhtiöt ja kaapelitelevisioyhtiöt. Jokainen määritteli omat vaatimuksensa seuraavalle ip-versiolle ja kommentoi ehdotuksia.

Ehdotuksista parhaimmaksi osoittautui SIP (Simple IP), josta tuli uuden ip-version perusta. SIPiä laajennettiin muiden ehdotusten ideoilla, ja uusi versio sai nimekseen SIPP (Simple IP Plus), josta tuli seuraavan internet protokollan perusta. Lopulta IETF numeroi uusimman version kuudeksi ja nimesi version ipv6:ksi. Numero viisi jäi välistä, kun kokeelliselle Stream Protocol – kokeiluprotokollalle myönnettiin numero viisi. (Comer 2002, 600 - 602.) Ipv6 standardoitiin vuonna 1998 liki seitsemän vuoden suunnittelutyön jälkeen (Kaario 2002, 109).

3.3 Ominaisuudet

Ipv6:een on sisällytetty paljon samoja ominaisuuksia, joita oli ipv4:ssa, kuten lohkoaminen ja lähdereititys. Jotta jotain eroa vanhaan olisi, ipv6 muuttaa muutamia yksityiskohtia. Tärkeimmät muutokset ovat pidemmät osoitteet, laajennettu osoitehierarkia, joustava otsikkorakenne, parannetut optiot, mahdollisuus protokollan laajentamiseen, automaattiset asetusmääritykset ja uudelleennumerointi sekä resurssien varaaminen. (Comer 2002, 602 - 603.)

Ehdottomasti tärkein ipv6:n muutos on pidemmät osoitteet. Ipv6:ssa 128 bitin osoitteen pituus mahdollistaa niin suuren osoiteavaruuden, että kaikkien osoitteiden käyttäminen tulevaisuudessa tuntuu mahdottomalta. Laajempi osoitehierarkia mahdollistaa uusien tasojen lisäämistä osoitehierarkiaan. Ipv6:n joustava otsikkorakenne on yhteensopimaton ipv4:n kanssa ja ipv6:n otsikkorakenteessa on monia valinnaisia otsikoita. Samoin ipv6 tarjoaa valinnaisia ohjaustietoja, jotka tarjoavat uusia ominaisuuksia ja niitä voidaan lisätä pakettiin. (Comer 2002, 602.)

Ipv6:n myötä siirryttään pois protokollasta, joka määrittää tarkkaan pakettien yksityiskohdat. IETF voi tarvittaessa muokata ipv6-protokollaa, jolloin voidaan lisätä uusia ominaisuuksia tai reagoida verkkolaitteen tai ohjelmiston muutoksiin. Automaattinen osoitteen konfigurointi mahdollistaa eristetyn verkon tietokoneiden konfiguroida itselleen ip-osoitteet ja aloittaa kommunikointi. Ipv6-protokollassa on kaksi uutta ominaisuutta, vuon käsite ja eriytettyjen palveluiden määritys, joilla voidaan varata verkon resursseja etukäteen. (Comer 2002, 603.)

Ipv6-protokolla keventää reitittimien taakkaa kieltämällä ip-pakettien pilkkomisen. Ip-pakettien pilkkominen tapahtuu verkon reunalla alkuperäisen lähettäjän toimesta. Ip-pakettien lohkoamisen kieltäminen asettaa ipv6-verkkojen linkeille haasteen, sillä niiden täytyy pystyä välittämään vähintään 1280 tavun pituisia ip-paketteja. Vastaava raja ipv4-verkossa on 68 tavua. (Kaario 2002, 109 - 110.)

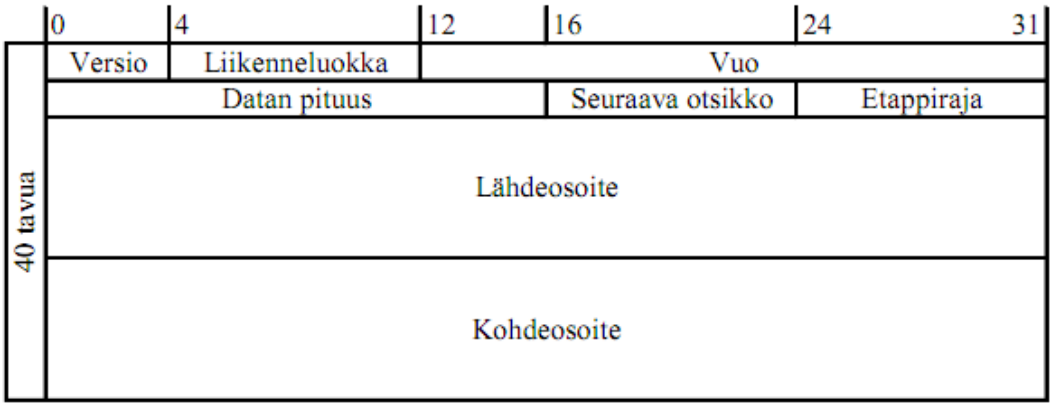
Ipv6-protokollassa on pyritty parantamaan tietoturvaa rakentamalla tietoturva osaksi protokollaa lisäämällä siihen pari tietoturvan lisäotsikkoa: todennus- ja salausotsikko. Todennusotsikko antaa vastaanottajalle mahdollisuuden varmistua paketin lähettäjästä otsikon lisäämän tarkistussumman avulla. Salausotsikko salaa paketissa olevan datan. Salausotsikko on viimeinen lisäotsikko ipv6-paketissa, koska salausotsikkokin on osittain salattu. Ipv6:n suojaus suojaa myös ylempiä protokollakerroksia. Ipv6-protokollalla voidaan parantaa reitittimien välistä yhteyttä ja luoda turvallinen yhdyskäytävä. (Kaario 2002, 122, 126.)

Ipv6:n yksi laajennusosa, mobile ipv6, tulee olemaan tulevaisuudessa kovassa käytössä langattomissa verkoissa mobiilien päätelaitteiden määrän kasvaessa. Mobile ipv6 sallii käyttäjän vaihtaa verkkoa ja pitää sama ip-osoite sekä avoinna olevat yhteydet. Mobile ipv6 käyttää samoja ipv6:n ominaisuuksia, kuten osoitteen automaattista asennusta ja lisäotsikoita. (Kaushik 2012.)

3.4 Kehysrakenne

Ipv6 muuttaa kehystä huomattavasti verrattuna ipv4:een. Ipv6:n kehyksessä on vakiomittainen, 40 tavua pitkä perusosa, valinnaisia laajennusosia ja lopuksi data. Kuviosta viisi huomataan, että ipv6:n kehys sisältää vähemmän pakollisia tietoja

kuin ipv4:n kehys. Jotkin ipv4-kehyksen otsikoista on siirretty ipv6:ssa laajennusotsikoiden alle, joita ei ole esitetty kuviossa viisi. Ipv6 on optimoitu toimimaan 64-bittisessä ympäristössä, jonka takia kehys on jaettu 64-bittisiin lohkoihin 32 bitin sijasta. (Comer 2002, 604; Kaario 2002, 109.)



KUVIO 5. Ipv6-kehyksen perusosa (Comer 2002, 604)

Ensimmäinen, looginen eroavaisuus versioiden kesken on versio-kentässä. Ipv4:ssa versio-kenttään tuli arvo neljä, ipv6:ssa versio-kenttä saa arvokseen kuusi. Muita kehyksien muutoksia versioiden välillä ovat otsikon ja datan pituudesta kertovat kentät. Nämä kentät on korvattu Datan pituus -kentällä. Datan pituus -kenttä kertoo 16 bitillä, montako tavua kehyksessä on peruskehyksen lisäksi. Perusosan pituuden ollessa aina vakio, kehyksen pituuskenttää ei tarvita erikseen kertomaan kehyksen pituutta. Lähde- ja kohdeosoitteiden kentät ovat 16 tavua pitkät. Etappiraja-kenttä korvaa elinikä-kentän. Etappiraja-kenttä kertoo paketin etappien määrän. Liikenneluokka-kenttä korvaa Palvelun tyyppi -kentän ja Liikenneluokka-kentän laajennus on Vuo-kenttä. Liikenneluokka-kenttää käytetään apuna reitityspäätöksiä tehdessä. Vuo-kenttää käytetään polun varaamiseen verkossa ja sillä tunnistetaan, mitkä paketit kuuluvat samaan loogiseen yhteyteen. Näin sovellukset voivat varata tietynlaiset vaatimukset täyttävän polun kahden tietokoneen välille. Seuraavan otsikon tyyppi on kerrottu omassa kentässä ja se korvaa Protokolla-kentän. Tarkistussumma-kenttä on poistettu kokonaan ipv6:sta, koska nykyään siirtotekniikat ovat luotettavampia.

Vastaavasti ylempien protokollien tarkistussumma on pakollinen. (Comer 2002, 604 - 605; Kaario 2002, 109.)

Suunnittelijat kehittelivät ipv6:een laajennusotsikot, jotta protokollan yleisyys ja tehokkuus paranisivat. Eri toiminnoille, kuten lohkoamiselle, lähdereititykselle ja laillisuustarkistukselle kiinteän paikan varaaminen peruskehyksestä olisi ollut huono ratkaisu, koska läheskään aina näitä ei käytetä. Lisäksi perusosaa oli karsittava, koska pitkät ipv6-osoitteet vievät paljon tilaa. Lähettäjä voi valita käytettävät laajennusotsikot ja laajennusotsikot toimivat samoin kuin ipv4:n optiot. Laajennusotsikot tuovat joustavuutta protokollaan. (Comer 2002, 605.)

Ipv6:ssa on lisäotsikoita kuusi kappaletta, joiden lukumäärä paketissa on valinnainen, mutta järjestys on määrätty. Otsikot ovat järjestyksessä: hyppyoptio-otsikko (Hop-by-hop Options Header), kohdeoptio-otsikko (Destination Options Header), reititysotsikko (Routing Header), lohkoamisotsikko (fragment header), todennusotsikko (Authentication Header), salausotsikko (Encapsulating Security Payload Header) ja uudestaan kohdeoptio-otsikko. Ensimmäinen kohdeoptio-otsikko sisältää tietoja, jotka halutaan välittää kohteen lisäksi kaikkiin matkan varrella vastaan tuleviin, reitityskentässä mainittuihin kohteisiin. Toinen kohdeoptio-otsikko välittää tiedot vain lopulliseen kohteeseen. (Kaario 2002, 115.)

Hyppyoptio-otsikkoa käyttämällä voidaan ip-paketissa kuljettaa tietoa, jota voidaan tutkia matkan varressa olevissa reitittimissä. Hyppyoptio-otsikko muodostuu kahdeksan bittiä pitkästä Seuraava otsikko-kentästä, kahdeksanbittisestä pitkästä Lisäotsikon pituus-kentästä ja loput 16 bittiä ovat Optioita, joiden määrä vaihtelee. Optiot ilmaistaan TLV-koodauksella (Type-Length-Value), jossa ensimmäinen kenttä kertoo option tyypin, toinen kertoo datan pituuden ja kolmas sisältää datan. (Kaario 2002, 117.)

Reititysotsikkoa käyttämällä voidaan pakottaa ipv6-paketti kiertämään tiettyjen verkon solmujen kautta kohteeseen. Reititysotsikko rakentuu kahdeksan bitin Seuraava otsikko -kentästä, kahdeksan bitin Lisäotsikon pituus –kentästä, kahdeksan bitin Reititystyyppi-kentästä ja kahdeksan bitin Solmuja jäljellä -kentästä. Lisäotsikon pituus -kenttä kertoo 64 bitin monikertana, kuinka pitkä

otsikko on. Ensimmäiset 64 bittiä jätetään huomioimatta. Jos Reititystyyppi-kentän arvo poikkeaa standardista, reitittimen on hylättävä kyseinen ipv6-paketti ja lähetettävä ICMP-viesti paketin lähettäjälle. Solmuja jäljellä -kenttä kertoo, kuinka monta solmua on vielä jäljellä ennen kuin paketti pääsee perille kohteeseen. Otsikon loppuosaan on varattu tilaa reititystyypille ominaiselle datalle. (Kaario 2002, 118 - 119.)

Lohkoamisotsikon toiminta on periaatteellisesti samanlaista kuin ipv4:ssa paketin lohkoaminen pienemmiksi paketeiksi. Ipv4:ssa paketti voitiin lohkoa pienemmiksi matkan varrella reitittimessä, jos jokin yhteys ei tue niin isoa pakettia. Ipv6:ssa paketin lohkoaminen matkan varrella reitittimissä on kielletty, koska lohkoaminen täytyy tapahtua heti lähetyksen yhteydessä. Tämä helpottaa ja nopeuttaa runkoreitittimien työtä. Ipv6-protokolla osaa tutkia ICMP-viesteillä verkon salliman paketin maksimipituuden, jolloin pakettien pitäisi olla aina sopivan kokoisia lähetykseen. Jos paketti onkin liian iso, lähettäjä saa ICMP-viestin liian isosta paketista ja samalla tiedon paketin suurimmasta sallitusta koosta. (Kaario 2002, 121.)

Ipv6:n tietoturvaa parantavat todennusotsikko ja salausotsikko. Todennusotsikon tehtävä on tarjota vastaanottajalle mahdollisuus varmistua paketin lähettäjästä. Todennusotsikko laskee useita parametrejä ja salausavainta käyttäen tarkistussumman ja lisää sen otsikkoon. Jos vastaanottaja pystyy generoimaan datasta samanlaisen tarkistussumman kuin otsikon tarkistussumma on, vastaanottaja voi olettaa, että lähettäjä on aito. Salausotsikko salaa ipv6-paketissa kulkevan datan. Salausotsikon tulee olla viimeisenä, koska sen jälkeen muut lisäotsikot ovat salattuja. Salausotsikon sisältämä turvallisuusindeksi ja järjestysnumero ovat salaamattomia, loput kentät ovat salattuja. Salaus- ja todennusotsikoita käytetään erillään, vaikka standardi ei suoraan kiellä niiden käyttämistä yhtäaikaa. (Kaario 2002, 122.)

3.5 Osoitteistus

Ipv6:n osoiteavaruus on huomattavasti laajempi kuin ipv4:n. Ipv4:n osoiteavaruus on 2^{32} ja ipv6:lla se on 2^{128}. Ipv4:n osoitteita on kappalemäärältään noin neljä

miljardia ja ipv6:n osoitemäärän voi ilmoittaa pyöristettynä 3,4* 10^{38}. Osoitteiden määrästä voidaan laskea kuvaavasti, kuinka kauan kestää käyttää kaikki ipv6:n tarjoamat osoitteet. Jos osoitteita varattaisiin miljardi kappaletta joka millisekunti, kestäisi kaikkien osoitteiden varaaminen yli 10^{18} vuotta. (Comer 2002, 610.)

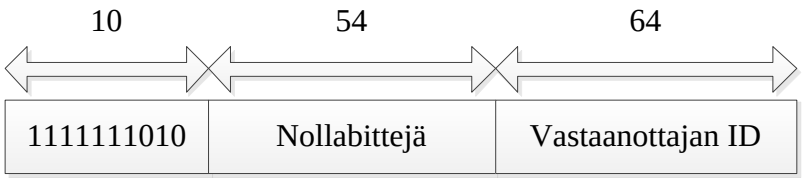
Laajentunut osoiteavaruus tuo mukanaan uuden ongelman. Ipv6-osoitteet ovat niin pitkiä, että ihmisen on hankala käsitellä ja muistaa niitä. Ipv4:n käyttämä pisteillä erotettu desimaalimuoto tekee pitkästä osoitteesta hankalasti luettavan. Sunnittelijat oivalsivat, että osoitteet täytyy esittää aivan eri tavalla kuin aiemmin. Osoitteet esitetään colon hex -menetelmällä, eli heksadesimaalimuodossa kaksoispisteillä erotettuina 16 bitin osiin. MAC-osoitteesta otettiin hieman mallia ja ipv6-osoite muistuttaa osittain mac-osoitetta, esimerkiksi 1F80:BAD8:3210:0:0:0:FF01:800. (Comer 2002, 610 - 611.)

Colon hex -menetelmä tuo ipv6-osoitteen esittämiseen pari sääntöä. Tavun ensimmäisen nollan voi jättää esittämättä, ja pelkkiä nollia sisältävät tavut voi lyhentää kahdella peräkkäisellä kaksoispisteellä. Edellä esitetyn osoitteen viimeinen tavu olisi loogisesti ”0800”, mutta säännön avulla siitä voidaan jättää ensimmäinen nolla pois, jolloin tavu kirjoitetaan ”800”. Toisella säännöllä osoitteen keskellä olevat nollat voidaan jättää pois ja korvata ne kaksoispisteillä, jolloin osoite olisi muodossa: 1F80:BAD8:3210::FF01:800. Kaksoispistelyhennystä saa käyttää vain kerran osoitteessa, jotta ei synny epäselvyyksiä. Colon hex -menetelmää käyttämällä voidaan ipv6-osoitteeseen lisätä pisteillä erotettu desimaalinen ipv4-osoite. Sekoitettuja osoitteita tullaan käyttämään siirtymäkauden aikana. Esimerkiksi ipv6-osoite 0:0:0:0:0:0:8.8.8.8 on validi osoite, joka lyhenee muotoon ::8.8.8.8. Ipv6:ssa voidaan merkitsevien bittien määrä ilmoittaa CIDR-tyylisesti kauttaviivalla ja kokonaisluvulla, kuten 12AB::CD30:0:0:0:0/60 määrittää osoitteen 60 ensimmäistä bittiä: 12AB00000000CD3. (Comer 2002, 611.)

Ipv6:ssa ip-osoite viittaa tiettyyn verkkoliityntään kuten ipv4:ssakin. Erona on se, että ipv6 sallii tietokoneen verkkoliitynnälle useita ip-osoitteita samanaikaisesti, jotta ip-osoitteiden määrittäminen ja muuttaminen olisi helppoa. Ipv6:ssa ei ole kiinteää ip-osoitteiden luokkajakoa, mutta runsas osoitteiden määrä mahdollistaa

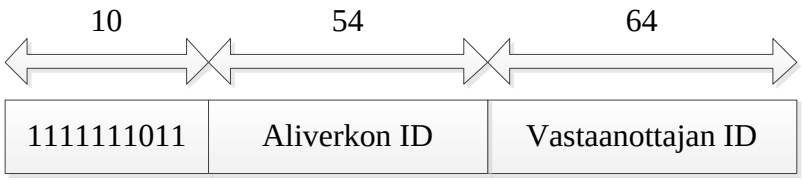
kolme perusosoitetyyppiä: unicast, anycast ja multicast. (Comer 2002, 612; Kaario 2002, 112.)

Unicast-osoitteet ovat tietokoneen tai reitittimen ip-osoitteita, joihin paketit on reititettävä lyhintä reittiä pitkin. Unicast-osoitteet jaotellaan globaaleiksi (global), aluekohtaisiksi (site local) ja linkkikohtaisiksi (link local). Linkkikohtaista ip-osoitetta voidaan käyttää vain yhdellä linkillä, eikä sitä saa reitittää muualle. Kuvio kuusi kertoo linkkikohtaisen osoitteen rakenteen. Ensimmäiset 10 bittiä ovat aina samat, näiden jälkeen tulee 54 kappaletta nollia ja lopuksi tulee vastaanottajan ID. Linkkikohtaisten osoitteiden alue on fe80::/10, mutta osoitteen nollabitit vievät tilaa, joten linkkikohtaisten osoitteiden alueeksi muodostuu fe80::/64. (Comer 2002, 612; Kaario 2002, 112; RFC 4291 2006.)



KUVIO 6. Linkkikohtaisen osoitteen rakenne

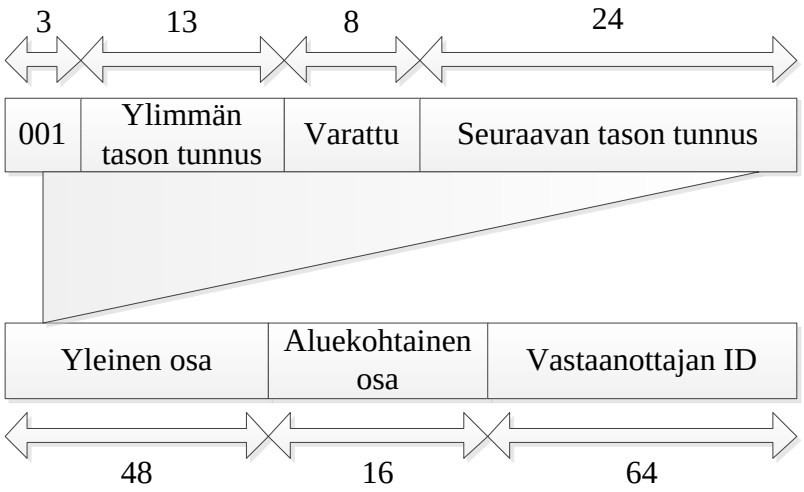
Aluekohtaisia osoitteita voidaan verrata ipv4:n yksityisiin osoitteihin. Aluekohtaiset osoitteet on suunniteltu käytettäväksi yksityisissä verkoissa, eikä niitä saa reitittää yksityisen alueen ulkopuolelle. Kuviosta seitsemän nähdään aluekohtaisen ip-osoitteen rakenne. Ensin tulee bittikuvio 1111111011, joka kertoo osoitteen olevan aluekohtainen. Sitten tulee aliverkon id 54 bitillä ja lopuksi vastaanottajan ID. (Kaario 2002, 112 - 113; RFC 4291 2006.)



KUVIO 7. Aluekohtaisen osoitteen rakenne

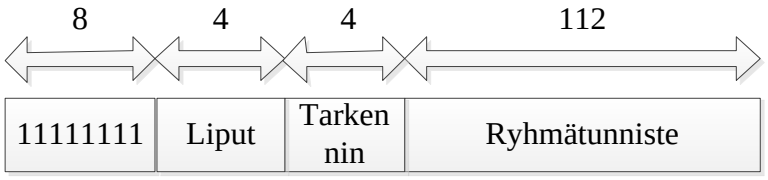
Globaali ipv6-osoite koostuu kolmesta osasta: yleisestä osasta, alueellisesta osasta ja vastaanottajan tunnistusosasta, joista yleinen osa muodostuu vielä pienemmistä osista. Yleinen osa on internetoperaattoreita ja palveluntarjoajia varten, joka tarjoaa datansiirtopalveluita muille. Aluekohtainen osa on tarkoitettu datansiirtopalveluiden käyttäjälle, esimerkiksi yrityksille. Aluekohtaisen osan tarvitsija ei tarjoa datansiirtopalveluita itsensä ulkopuolelle, esimerkiksi yritys ei tarjoa yhteyksiä muille. (Kaario 2002, 113.)

Yleisen osan muodostaa osoitteen 48 ensimmäistä bittiä (kuviossa kahdeksan alempi rakennekuva). Kuviossa kahdeksan on esitetty globaalin ip-osoitteen rakenne. Ylimmän tason tunnus (Top-Level Aggregation Identifier, TLA ID) kertoo, mikä elin huolehtii kyseisten tunnusten jakamisesta. Mitä korkeamman tason tunnus, sen korkeampi elin on vastuussa tunnuksista. Varatut 8 bittiä ovat varalla tulevaisuuden käyttöä varten. Seuraavan tason tunnusta (Next-Level Aggregation Identifier, NLA ID) organisaatio käyttää luodakseen osoitehierarkian ja tunnistaakseen sivustoja. Alueellinen tunnus (Site-Level Aggregation Identifier, SLA ID) on 16 bittiä pitkä ja se on hierarkian alin taso. Edellä mainitut hierarkiat voidaan jakaa sisäisesti vielä pienempiin osiin, jotta saadaan protokollaan lisää joustavuutta. Paketin vastaanottaja tunnistetaan ipv6-osoitteen viimeisistä 64 bitistä, joka on yhteistä kaikille globaaleille ipv6-osoitteille. (RFC 2450 1998; Kaario 2002, 113.)



KUVIO 8. Globaalin ip-osoitteen rakenne

Kuviosta yhdeksän nähdään ipv6:n multicast-osoitteen rakenne. Ipv6:n multicast-osoite alkaa aina kahdeksalla ykkösbitillä. Lippubiteistä kolme vasemmanpuoleista ovat nollia ja viimeisellä bitillä ilmaistaan, onko osoite väliaikainen vai pysyvä. Arvolla nolla se on yleisesti tunnettu ja pysyvä, kun taas arvolla yksi multicast-osoite on väliaikainen. Tarkennin-biteillä kerrotaan, minkä ryhmän multicast-lähetys on kyseessä. Ryhmätunniste kertoo, mille ryhmälle multicast-lähetys on osoitettu. (Kaario 2002, 114; RFC 4291 2006.)



KUVIO 9. Ipv6:n multicast-osoitteen rakenne

Anycast-osoite on ipv6:n tuoma uudistus ip-verkkoon. Anycastin ideana on, että useampi laite muodostaa anycast-ryhmän. Yleensä ryhmän laitteet tarjoavat samaa palvelua, esimerkiksi samaa palvelua tarjoavat palvelimet. Palvelimet eivät käytä keskenään liikennöintiin anycast-osoitetta, vaan asiakaskoneet kyselevät palvelua anycast-osoitteella. Kun reititin havaitsee anycast-paketin, se välittää paketin jollekin anycast-ryhmään kuuluvista palvelimista. Kun paketti lähetetään kyseiseen ryhmään, joku ryhmään kuuluva laite vastaanottaa paketin. Anycast-osoitteen rakenne on samanlainen kuin unicast-osoitteen. (Kaario 2002, 115,122 - 123, RFC 4291 2006.)

Ipv6:ssa tuetaan Plug-and-Play -tyylistä osoitteiden asentamista, jolloin käyttäjän ei tarvitse tehdä ip-osoitteiden asentamisen vuoksi mitään. Automaattinen asentaminen voidaan tehdä tilattomasti (stateless autoconfiguration) tai tilallisesti (stateful autoconfiguration). Tilanton asentaminen on ipv6:n mukana tullut uudistus, jota ei ollut ipv4:ssa. Tilattomassa asennuksessa tietokone tai jokin muu päätelaite voi verkkoon liityttyään generoida itse itselleen ip-osoitteen ilman kontrolloitua hallintaa. Tilallisessa asentamisessa tietokone tai päätelaite ottaa yhteyden palveluun, esimerkiksi DHCPv6-palvelimen tarjoamaa, ja saa palvelusta

kokonaisen osoitteen, kuten ipv4:ssa käytettäessä DHCP-palvelua. (Kaario 2002, 123.)

Tilattoman asennuksen mahdollistaa linkkikohtaiset osoitteet ja sulautetut liityntöjen osoitteet. Tietokone luo ip-osoitteen kuten kuviossa kuusi, eli alkuun ensimmäiset 10 bittiä ovat linkkikohtaisen osoitteen bittikuvio 1111 1110 10. Tämän jälkeen lisätään 54 nollabittiä ja lopuksi tietokoneen oman liitynnän 64-bittinen tunniste. Linkkikohtaisen osoitteen käyttökelpoisuus varmistetaan lähettämällä reitittimelle router solicitation -sanoma, jolla pyydetään lisätietoa. Jos samassa verkossa on reititin, reititin vastaa lähettämällä router advertisement -sanoman. Sanomassa käy ilmi, mitä etuliitteitä tietokone voi käyttää toimipaikkakohtaisissa ja yleisissä osoitteissa sekä voiko automaattisesti luotua osoitetta käyttää vai onko osoite pyydettävä DHCPv6-palvelimelta. Tietokone asettaa sanomaan vastanneen reitittimen oletusreitittimikseen. (Comer 2002, 620, Kaario 2002, 124.)

Ipv6-protokolla sallii reitittimien rajoittaa antamiensa tunnusten käyttöaikaa, jotta verkkojen uudelleennumerointi voitaisiin toteuttaa. Reitittimen router advertisemen –sanoma sisältää myös tiedon ehdottoman voimassaolonajasta ja suositellusta voimassaoloajasta. Suositetun voimassaoloajan jälkeen tietokoneen etuliite on edelleen kelvollinen, mutta sen on käytettävä toista etuliitettä kaikessa kommunikoinnissa aina, kun se on mahdollista. Tietokoneen on lopetettava itsekehittämän etuliitteen käyttö, kun ehdoton voimassaoloaika täyttyy, vaikka yhteyksiä olisi avoinna. (Comer 2002, 620.)

Tilallisessa asennuksessa asiakastietokone muodostaa ensin linkkikohtaisen osoitteen, kuten tilattomassakin asennuksessa (Kaario 2002, 125). DHCPv6:ssa on kaksi erilaista keskustelumenetelmää asiakkaan ja palvelimen välillä: neljän viestin vaihto ja kahden viestin vaihto. Neljän viestin vaihtoa käytetään, kun asiakas haluaa ipv6-osoitteen ja muita parametrejä. Tämä on melko vastaava DHCPv4:n kanssa. Ensin asiakas lähettää multicastilla Solicit-viestin löytääkseen DHCPv6-palvelimen. Seuraavaksi kaikki palvelimet, jotka täyttävät asaikkaan vaatimukset, vastaavat Advertise-viestillä. Kolmannessa vaiheessa asiakas valitsee itselleen sopivat palvelimen ja lähettää Request-pyynnön saadakseen

osoitteen ja muita parametrejä. Lopuksi palvelin vastaa Reply-viestillä ja asiakas saa ip-osoitteen. Lyhyemmässä versiossa asiakas lähettää Solicit-viestin ja palvelin vastaa Reply-viestillä, jossa tulee parametrit. (The TCP/IP Guide 2005.)

3.6 Ipv4:n ja Ipv6:n eroavaisuudet

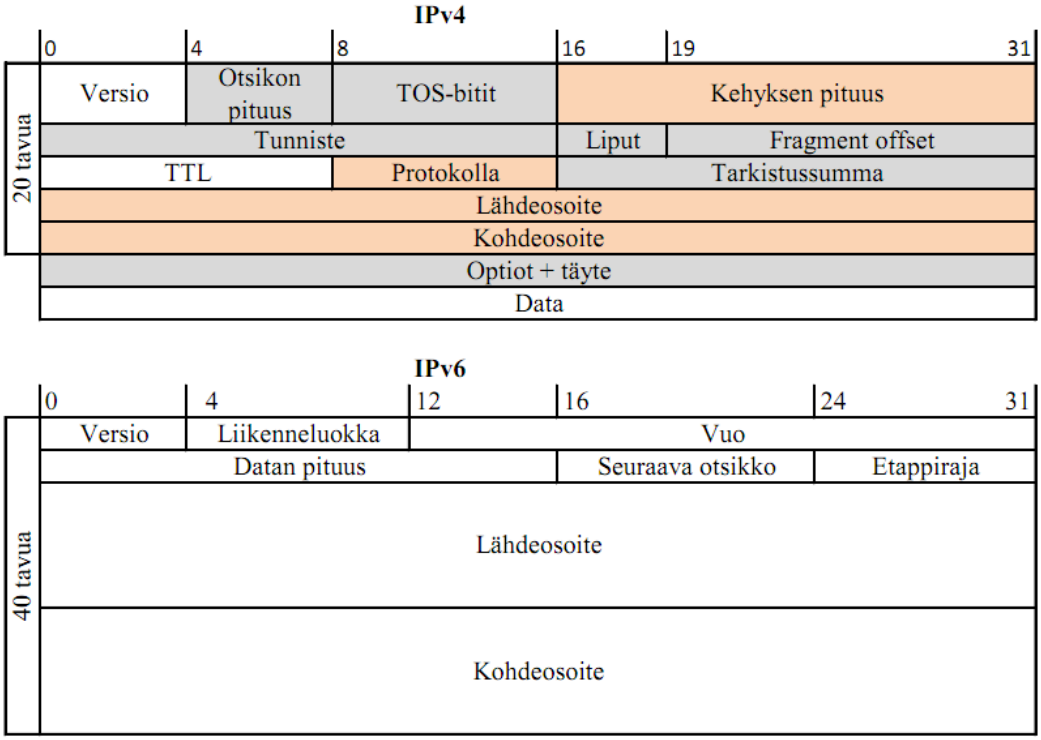
Ipv4- ja ipv6-protokollien välillä on pieniä ja suuria eroavaisuuksia, joita voidaan tarkastella taulukosta kolme. Suurimmat muutokset ovat ip-osoitteiden määrä, esitysmuoto, osoitehierarkia ja kehykset. Ip-osoiteavaruudet nelinkertaistuminen ipv6:ssa mahdollistaa luopumisen NAT:sta ja muista vastaavista tekniikoista. Esitysmuodon vaihtuminen desimaalimuodosta heksadesimaalimuotoon tekee osoitteet vaikesti luettaviksi, mutta lyhentää osoitteita. Ipv6:ssa ei tarvita maskia erottelemaan verkko-osaa laiteosasta, kuten ipv4:ssa. Ipv4:ssa käytetään maskia erottelemaan aliverkot. Ipv6:ssa aliverkon tunniste on ip-osoitteessa, joilloin maskia ei tarvita kertomaan aliverkkoa vaan osoitteen etuliitettä. Osoitteen etuliite kertoo, montako bittiä osoitteen alusta käytetään aliverkon tunnistukseen.

TAULUKKO 3 Vertailu ipv4:n ja ipv6:n kesken (Cisco 2012, IBM 2012)

Ominaisuus	**Ipv4**	**Ipv6**
Osoitteet	32-bittiset, 4 tavua	128-bittiset, 16 tavua
Osoitteen rakenne	Koostuu verkko- ja laiteosasta, vaihtelevat luokan tai maskin mukaan	Koostuu 64-bittisestä verkko-osasta ja 64-bittisestä asiakasosasta
Osoitteen esitysmuoto	Desimaalimuoto, xxx.xxx.xxx.xxx, 0<=x<=255	Heksadesimaalimuoto, xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx, 0<=x<=15 (F)
Osoitteen maski	Käytetään verkko- ja laiteosan erottamiseen	Ei käytetä
Osoitteen etuliite	Desimaalimuoto tai /xx-muoto	Kertoo aliverkon osan ip-osoitteesta. /nnn, 0<=n<=128
Aliverkotus	Aliverkot tunnistetaan maskilla	Aliverkot tunnistetaan ip-osoitteesta
Osoitetyypit	Unicast, multicast ja broadcast	Unicast, multicast ja anycast
Yksityiset osoitteet	10 /8, 172.16 /12 ja 192.168/16. Ei voi reitittää internetiin	Aluekohtaiset osoitteet vastaavat yksityisiä osoitteita
Loopback-osoite	127.0.0.1	::1

Osoitteen konfigurointi	Käsin konfigurointi tai DHCP	Tilaton autokonfigurointi tai tilallinen DHCPv6
Lohkoaminen	Lohkoaminen sallittu matkan varrella	Vain lähettäjän toimesta
Ip kehys	Vaihtuva pituus, 20 - 60 tavua	Kiinteä pituus 40 tavua, normaalisti lyhyempi kuin ipv4-kehys
Ip kehyksen optiot	Sisällytetään kehykseen ennen dataa	Ei optioita, vastaavat ovat lisäotsikoita
NAT	Käytetään reitittimissä ja palomuureissa	Ei käytetä

DHCPv6 toimii pääpiirteittäin samoin kuin DHCPv4, mutta niissä on myös paljon eroavaisuuksia. DHCPv6:ssa on luovuttu BOOTP:stä sen nykyajan vähäisen käytön takia. DHCPv6 on parempi, koska sen linkkikohtaista osoitetta käytetään DHCPv6-palvelimen hakemiseen ja oikean ip-osoitteen kysymiseen. Kaikki Ipv6-järjestelmät tukevat multicastia. Kaikki DHCPv6-palvelimet ottavat vastaan multicast-paketit ja verkko tietää, mihin lähettää DHCP-kyselyt. Ipv4:ssä asiakkaat mainostavat kyselyjään eikä verkko tiedä miten kauas kyselyt täytyy lähettää. DHCPv6 sallii normaaleiden ja väliaikaisten osoitteiden jakamisen. DHCPv4:lla on enemmän optioita, joita jakaa asiakkaille. (Kerr 2006.)



KUVIO 10. Ipv4:n ja ipv6:n kehyksien otsikkokenttien erot (Kaario 2002, 110)

Kuviosta kymmenen nähdään, miten ip-kehyksien otsikot ovat muuttuneet. Kuvion ylempi kehys on ipv4:n ja alempi ipv6:n. Ipv4:n kaksitoista pakollista otsikkokenttää ja vaihtelevan mittaiset optiokentät on jätetty pois ipv6:sta ja siinä on vain kahdeksan pakollista kenttää, jonka lisäksi voidaan vielä ketjuttaa lisäotsikoita. Harmahtavalla pohjalla olevat Otsikon pituus-, TOS-bitit-, Tunniste-, Liput-, Fragment offset-, Tarkistussumma- ja Optiot + täyte -kentät on poistettu ipv6:sta. Punertavalla pohjalla olevat Kehyksen pituus-, Protokolla-, Lähdeosoite- ja kohdeosoitekentät ovat muuttuneet ipv6:ssa. Versio-kentän arvo riippuu käytettävän protokollan versiosta. Ipv4-protokolla saa arvoksi neljä ja ipv6 saa arvoksi kuusi. Otsikon pituus- ja Kehyksen pituus -kentät on korvattu Datan pituus-kentällä ipv6:ssa. Ketjuttamisen avulla ipv6-kehys on joustavampi ja muuntautumiskykyisempi kuin ipv4:n kehys. Ipv6:n kehysrakenne on suunniteltu 64-bittiseen arkkitehtuuriympäristöön, toisin kuin ipv4, jonka kehykset tasataan 32 bittiin. Lähde- ja kohdeosoitekentät vievät ipv6:ssa paljon tilaa, koska ip-osoitteet ovat niin suuret ipv4:n ip-osoitteisiin nähden.

3.7 Siirtymistekniikat

3.7.1 Yleistä siirtymistekniikoista ja siirtymisessä huomioitavia asioita

Siirtymistä ipv6:een ei voida tehdä yhdessä päivässä, vaan se on pitkän ajan prosessi, jonka takia joudutaan käyttämään erilaisia siirtymismenetelmiä ja tekniikoita. Siirtymisvaiheessa voidaan käyttää useita eri tekniikoita, kuten Dual stack -tekniikkaa, tunnelointia ja protokollan muunnosta. Dual stack -tekniikassa tietokoneet, palvelimet ja verkon laitteet käyttävät molempia protokollia riippuen siitä, miten kohde tukee protokollia. Tunneloinnissa ipv6-paketit enkapsyloidaan ipv4-paketin sisään ja lähetetään ipv4-verkon kautta ipv4-protokollaa käyttävälle kohteelle. Protokollan muunnos mahdollistaa vain ipv6-protokollaa käyttävän asiakaskoneen muodostaa yhteys vain ipv4-protokollaa käyttävän koneen kanssa.

Ennen ipv6-protokollan käyttöönottoa pitää varmistaa palvelimien, palveluiden, ohjelmistojen ja verkon laitteiden ipv6-tuki. Tämä voi olla työläs vaihe riippuen verkon koosta ja laitteiden sekä sovellusten määrästä. Muutaman vuoden ikäisissä ohjelmistoissa on usein tuki ipv6-protokollalle. Ipv6:een siirtyminen alkaa olla jo niin ajankohtainen asia, että viimeistään ohjelmistojen nykyisissä versioissa ipv6-tuki on tai on tulossa.

3.7.2 Dual stack

Dual stack on tekniikka, joka tarjoaa täydellisen tuen molemmille ip-protokollille. Ipv6-laitteita, jotka tukevat molempia protokollia, kutsutaan ipv6/ipv4 -laitteiksi ja nämä laitteet voivat liikennöidä käyttäen ipv4- tai ipv6-osoitetta. Laitteilla, kuten reitittimellä ja tietokoneella, voi olla käytössä erikseen tai yhtäaikaa molemmat protokollat. Jos laitteen ipv6-protokolla on poissa käytöstä, se käyttäytyy kuten ipv4-protokollaa käyttävä laite. Jos taas laitteen ipv4-protokolla on poissa käytöstä, se käyttäytyy kuten ipv6-protokollan laite. Ipv6/ipv4 -laite voi tukea käsin konfiguroitua tunnelia, automaattisesti konfiguroitua tunnelia tai olla kokonaan tukematta tunneleita. (RFC 2893 2000.)

Ipv6/ipv4 -laite saa molemmat osoitteet, ipv4-osoitteen laite saa esimerkiksi DHCP:ltä ja ipv6-osoitteen laite saa tilattomattomalla konfiguroinnilla tai DHCPv6:lla (RFC 2000). Ipv6 on prioriteetiltään arvokkaampi, jolloin laitteen saadessa molemmat ip-osoitteet, laite käyttää ensisijaisesti ipv6-osoitetta asioidessaan sivustoille, jotka tukevat ipv6-osoitteita.

Dual stack -tekniikan käyttöä saattaa rajoittaa sovellusten tuki. Vain ipv4-protokollalle suunnitelluissa sovelluksissa API (Application programming interface) voi olla koodattu tukemaan vain ipv4-osoitteita. Kun sovellusta on kehitetty tukemaan sekä ipv4- että ipv6 -protokollia, sovelluksen API osaa käsitellä ipv6-protokollan 128-bittisiä osoitteita ja sovellus voi käyttää liikennöintiin ipv4- tai ipv6 -protokollan osoitteita. (Desmeules 2007, 228.)

3.7.3 6to4

6to4-tunnelointitekniikka on tilaton, automaattinen tunnelointitekniikka, joka mahdollistaa ipv6-protokollan käyttämisen ipv4-verkossa muodostaen dynaamisen tunnelin. 6to4-tunnelointia varten asiakaskone tarvitsee julkisen ipv4-osoitteen ja asiakaskoneelle konfiguroidaan ipv4-osoite 192.88.99.1, joka on asiakasta lähimpänä olevan 6to4-välitysreitittimen anycast-osoite. Asiakaskone lähettää ulospäin lähtevät ipv6-paketit tuohon osoitteeseen, josta välitysreititin lähettää paketit eteenpäin ipv4-verkossa. Vastauspaketit palvelimelta tulevat yleensä eri reittiä, koska palvelimen lähin 6to4-välitysreititin on yleensä eri kuin asiakkaan lähin välitysreititin. (Linux 2011; The ipv6 portal 2012.)

Laitevalmistajat pyrkivät jättämään 6to4-tunneloinnin oletuksena pois päältä, koska 6to4-tunnelointi on vikaherkkä. 6to4-tunneloinnin vikaherkkyyttä on testattu liikennöimällä tunnelin kautta dual stack- ja vain ipv6-kohteisiin. Epäonnistumisprosentti on pyörinyt 15 prosentin paikkeilla, joka on aika suuri epäonnistumisprosentti. Kun 6to4-tunneli epäonnistuu yhteydenotossa, kestää hetki ennenkuin asiakaslaite yrittää yhteyttä uudelleen ipv4:lla. Tämä hidastaa internetin käyttöä ja aiheuttaa käyttäjille huonoja kokemuksia. On suositeltavaa kytkeä 6to4-tunnelointi pois päältä Windows Vistassa ja uudemmissa käyttöjärjestelmissä, joissa se on oletuksena päällä. On suositeltavaa siirtyä

suoraan käyttämään ipv6:sta omissa sisäverkoissa, jolloin vältytään monenlaisten rikkinäisten muunnostekniikoiden käytöltä. (Aben 2010, 2011.)

3.7.4 Tunnel broker -tunnelointi

Tunnel broker tarjoaa vaihtoehtoisen tavan siirtyä ipv6:een. Tunnel broker perustuu Tunnel broker -palvelimiin, jotka käsittelevät asiakkailta tulevia tunnelipyyntöjä. Tunnel broker hallitsee tunnelin luonnin, muutoksien teon ja poistamisen asiakkaan puolesta. Tunnel brokerin odotetaan olevan hyödyllinen kun ipv6-asiakkaiden määrä kasvaa ja se auttaa ipv6-palveluntarjoajia tarjoamaan helpon pääsyn heidän ipv6-verkkoon. (RFC 3053 2001.)

Tunnel broker -ja 6to4-tekniikka eroavat toisistaan jonkin verran. Tunnel broker sopii hyvin pienille eristetyille ipv6-sivustoille ja varsinkin eristetyille ipv6-asiakkaille, jotka ovat ipv4-verkossa ja haluavat yhdistää olemassaolevaan ipv6-verkkoon. 6to4 on suunniteltu tarjoamaan eristetyille ipv6-sivustoille helpon tavan yhdistää ne yhteen ilman palvelutarjoajan ipv6-natiivipalveluita. 6to4 sopii hyvin extranet- ja virtuaalisten privaattiverkkojen käyttöön. (RFC 3053 2001.)

Tunnel broker -käyttäjät ovat ipv6-dual stack -käyttäjiä, jotka ovat ipv4-verkossa. Käyttäjä varmennetaan Tunnel broker -palvelimelle ja käyttäjän täytyy tarjota palvelimelle tiettyjä tietoja ja palvelin hoitaa konfiguroinnin osoitteiden, kuormanjaon ja DNS:n suhteen. Konfiguroinnin jälkeen yhteys toimii ja sallii tunnel broker -käyttäjän liittyä ipv6-verkkoon, johon Tunnel broker -palvelin on yhteydessä. (RFC 3053 2001.)

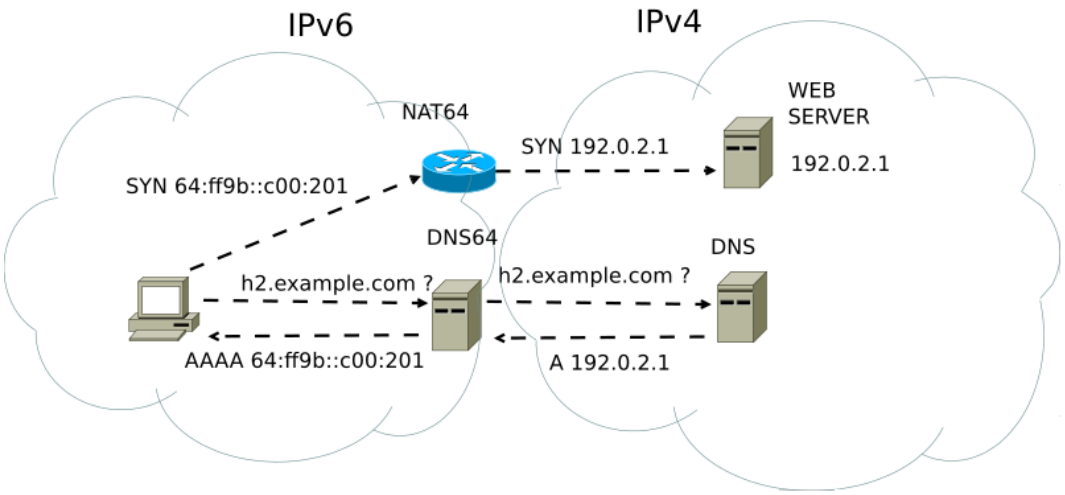
3.7.5 ISATAP

ISATAP on automaattinen tunnelointitekniikka, jota käytetään ipv6-unicastyhteyksiin ipv6/ipv4-laitteiden välillä ipv4-intranetissä. ISATAP tunneloi automaattisesti host-to-host-, host-to-router- ja router-to-host -välisen liikenteen. ISATAP-laitteet eivät tarvi mitään manuaalista konfigurointia, ja ne voivat luoda ISATAP-osoitteen käyttäen tavallista osoitteen automaattista konfigurointia. (Davies 2008.)

ISATAP-osoitteet käyttävät paikallisesti hallinnoitua tunnistetta FE80::5EFE:q.w.e.r, jossa q.w.e.r on privaatti ipv4-unicast-osoite tai FE80::200:5EFE:q.w.e.r, jossa q.w.e.r on julkinen ipv4-unicast-osoite. ISATAP-osoitteessa voi olla mikä tahansa 64-bittinen etuliite, joka on validi ipv6-unicast-osoite. ISATAP-osoitteessa on sisällä ipv4-osoite, jota käytetään kohdeosoitteena, kun ISATAP-osoitteinen ipv6-liikenne tunneloidaan ipv4-verkon läpi. (Davies 2008.)

3.7.6 NAT64/DNS64

Ipv4- ja ipv6-verkot ovat keskenään yhteensopimattomia. Tämän takia tarvitaan NAT64/DNS64-tekniikkaa, joka mahdollistaa liikennöinnin ipv4- ja ipv6-verkkojen välillä ilman dual stack -menetelmää. NAT64:ssa käytetään laitetta, jolla on omat liitynnät ipv4- ja ipv6-verkkoihin. NAT64-laite vastaanottaa ipv6-verkosta paketin, joka on suunnattu ipv4-verkkoon ja tekee paketille osoitteenmuutoksen niin, että paketti muuttuu ipv4-paketiksi ja se voidaan lähettää ipv4-verkossa olevalle vastaanottajalle. DNS64-palvelin toimii ipv6-asiakaskoneen ja normaalin DNS-palvelimen välissä. Kuviosta yksitoista nähdään, kuinka DNS64-palvelin sieppaa asiakaskoneelta tulevan DNS-kyselyn ja kysyy itse DNS:ltä kyseisen nimen ipv4-osoitteen. Saatuaan ipv4-osoitteen DNS64-palvelin muuttaa ipv4-osoitteen ipv6-osoitteeksi ja lähettää vastauksen asiakaskoneelle, joka ottaa yhteyttä kohteeseensa NAT64-laitteen läpi. Jos ipv6-verkosta saapuva paketti on menossa eri ipv6-verkkoon, se ohittaa NAT64-toiminnon. (Cisco 2008; Tuminauskas 2011;Ecdysis 2012.)



KUVIO 11. NAT64/DNS64-menetelmän toimintaperiaatekuva (Tuminauskas 2011)

3.7.7 Siirtymistekniikoiden vertailu

Siirtymistekniikoita on monenlaisia, joista pitää valita omaan verkkoon sopivin vaihtoehto. Eri sivustoilla suositellaan eri tekniikan käyttämistä, joten verkon ylläpitäjä joutuu pohtimaan, mitä tekniikkaa käytetään. Tunnelointitekniikat voivat aiheuttaa ylimääräistä työtä tunneleiden luomisen takia. 6to4-tekniikka on vikaherkkä, ja se jätetään oletuksena pois päältä. Tunnel broker -tekniikassa liikenne kulkee ulkopuolisen palvelimen kautta, joka voi olla tietoturvariski.

TAULUKKO 4. Siirtymätekniikoiden vertailu (Sellers 2009).

Siirtymätek-niikka	Edut	Haitat/ongelmat
Dual Stack	Voidaan käyttää ipv4:n rinnalla, ipv4:n lisäksi saadaan ipv6-toiminnallisuus. Helppo käyttää ja konfiguroida, joustava.	Voi vaatia kaksi reititystaulua, kuormittaa CPU:ta ja muistia.
6to4	Helppo käyttää ipv4-verkossa sijaitseville ipv6-saarille. Hyvä ipv6-domaineille, joilla ei ole ipv6-tukea.	Tarvitsee yhden julkisen ipv4-osoitteen ja 6to4-reitittimen. Ongelmia eristetyn ipv6-verkon ja ipv6-internetin välillä. Työläs konfiguroida.
Tunnel	Mahdollistaa käyttäjiltä tulevien ipv6-tunnelikyselyjen	Vaatii erityishuomiota turvallisuuden kanssa. Ei

Broker	hallinnan. Operaattori voi helposti säätää käyttäjien verkonkäyttöä.	välttämättä toimi, jos asiakas sijaitsee NAT:n takana. Ovat yleensä ulkopuolisia palvelimia.
ISATAP	Helppo ottaa käyttöön intranet:ssä. Tukee monia alustoja.	Tietoturvaongelmia. Suunniteltu intranet-käyttöön. Voi vaatia enemmän konfigurointia kuin muut tekniikat. Vian paikallistaminen hankalaa.
NAT64/ DNS64	Ipv6-verkoista mahdollista liikennöidä ipv4-verkkoon.	Vaatii tehokkaan NAT-laitteen.

Taulukossa neljä vertaillaan eri siirtymistekniikoiden hyviä ja huonoja puolia. Dual stack -teknikka on helppokäyttöinen, koska ipv6-osoitteet toimivat ipv4-osoitteiden rinnalla yhtäaikaa. Konfiguroinnin kannalta laitteisiin täytyy vain lisätä laitteille varatut ipv6-osoitteet. Haittapuolena lisääntyneiden osoitteiden määrä kasvattaa reititystauluja. Kasvavat reititystaulut kuormittavat enemmän reitittimien prosessoreita sekä keskusmuistia.

6to4, Tunnel broker ja ISATAP ovat automaattisia tunnelointitekniikoita. Tunnelointitekniikoille on yhteistä ipv6-pakettien enkapsylointi ipv4-paketin sisään. 6to4-tekniikka on helppokäyttöinen tilanteissa, joissa ipv6-saari sijaitsee ipv4-verkossa. 6to4-tekniikan konfigurointi reitittimeen on työlästä, koska reitittimeen täytyy määritellä käytettävä ipv6-osoite, liitynnät ja tunnelin tyyppi sekä linkin vastapäässä olevaan reitittimeen samat komennot.

Tunnel broker -tekniikan odotetaan olevan hyödyksi kun operaattorit alkavat tekemään massasiirtoja ipv4:sta ipv6:een. Tunnel broker sopii hyvin yksittäisille ipv6-asiakkaille, jotka ovat ipv4-verkossa ja haluavat liikenneöidä ipv6-verkkoon. Tunnel broker -tekniikassa asiakas rekisteröityy tunnel broker-palvelun tarjoajalle ja saa sieltä ohjeet sekä skriptin, jolla hoidetaan asennus omalle koneelle. Tämän jälkeen asiakkaan tietokone ottaa itsenäisesti yhteyden tunnel broker -palvelimeen asioidakseen ipv6-sivustolle ipv4-verkon kautta.

ISATAP:n konfigurointi tietokoneelle on varsin yksinkertaista. ISATAP otetaan käyttöön tietokoneessa, ja tietokone kehittää itse itselleen link local- ja julkisen

osoitteen lisäämällä ipv6-osoitteen loppuun oman ipv4-osoitteensa. ISATAP-tekniikkaa käytettäessä vianetsintä voi olla hankalaa. NAT64/DNS64 on muunnostekniikka, jossa käytetään muunnokseen soveltuvaa verkkolaitetta, joka on yhteydessä ipv4- ja ipv6-verkkoihin. NAT-tekniikan käyttöä ei suositella sen epäkäytännöllisyyden vuoksi ja koska NAT-muunnokset vaativat tehokkaan verkkolaitteen.

PHKK on päättänyt valita tähän työhön testattavaksi Dual stack -siirtymistekniikan sen yksinkertaisuuden vuoksi. Dual stack:a käytettäessä laitteita konfiguroidaan samoin kuin ennenkin, eikä verkosta tule monimutkaista tunneleiden eikä muunnostekniikoiden takia. Palomuurisäännöissä riittänee ipv4-sääntöjen kopiointi ja kopioitujen sääntöjen osoitteiden muuttaminen ipv6-osoitteiksi. Kahden protokollan käyttäminen tietysti lisää hieman ylläpidon töitä, kun palomuurisääntöjä on kahdet sekä verkon suunnittelussa ja toteutuksessa täytyy käyttää kahta eri protokollaa.

4 PHKK:N PALVELUIDEN JA PALVELIMIEN IPV6-TUKI

4.1 Palvelinalustojen ja käyttöjärjestelmien ipv6-tuki

Ipv6-tuki on oletuksena päällä seuraavissa Windows-versioissa: Windows 7, Windows Server 2008 R2, Windows Vista, Windows Server 2008, Windows Server 2003, Windows XP Service Pack 2, Windows XP Service Pack 1 ja Windows XP Service Pack 1:stä eteenpäin. Windows 7 ja Vista tukevat automaattisesti ipv6:sta käyttäen dual ip layer stackia. (Sourcedaddy 2012.) Windows 2000- ja 2003 -palvelimet eivät sisällä nykyistä ipv6-standardia, mikä aiheuttaa sen, että Windows 2003:lla pyörivät AD:t (Active Directory) pitäisi siirtää vähintään Windows Server 2008 -versioon tai mieluiten uusimpaan Windows Server 2008 R2 -versioon. (Morimoto 2011.)

Linux-kernelit ovat osittain tukeneet ipv6:sta jo versiosta 2.2.x asti. On kumminkin suositeltavaa käyttää vähintään kernel-versiota 2.4.x, koska vanhemman kernel-version ipv6-tuki ja -ominaisuudet voivat olla puutteelliset, rajalliset ja rikkonaiset. Parhaimman ipv6-tuen saa, kun siirtyy vanhemmista kernel-versioista käyttämään vähintään versiota 2.6.x ja sitä uudempia. (Bieringer 2009.)

Wmware ESX:n tuki ipv6-protokollalle alkaa versiosta 3.5, joka tukee ipv6-osoitteiden konfiguroinnin virtuaalikoneille. ESX:n versio neljä tukee ipv6-protokollaa ja sen lisäksi koekäytössä on ipv6:lla toteutettu levynjako. Versiossa neljä on myös tiettyjä ominaisuuksia, joita ei tueta ipv6:lle, kuten TCP segmentation offload ja Wmwaren vikasietoisuusominaisuudet. Oletuksena ipv6-protokolla ei ole käytössä. (Wmware 2011.)

4.2 Palvelut

HTTP & HTTPS

Apache tukee ipv6-protokollaa versiosta 2.0 lähtien (The Apache Software Foundation 2012). Microsoftin Internet Information Services (IIS) tukee ipv6-protokollaa versiosta 6.0 lähtien, mutta IIS 6.0:n kaikki omaisuudet eivät tue ipv6-

protokollaa, sillä ainoastaan WWW-palvelut tukevat ipv6-protokollaa. (Microsoft TechNet 2012.) IIS 7.5:ssa FTP-tiedonsiirto on tuettu, jota IIS 6.0 ei tukenut.

Microsoft Exchange

Microsoft Exchange 2007 SP1 ja SP 2 tukevat ipv6-protokollaa vain, jos Exchange on asennettu Windows Server 2008 -palvelimeen, jossa on ipv4- ja ipv6-protokollat käytössä. Jotkin Exchange 2007:n komponenteista eivät tue ipv6-protokollaa. (Microsoft 2011a.) Parannuksia ei ole Exchange 2010-versiossa tehty juurikaan, joten siihen pätee samat ehdot kuin Exchange 2007:aan. Puhdasta ipv6-ympäristöä ei vielä tueta. (Microsoft 2011b.)

Moodle

Kurssinhallinta- ja verkko-opetusjärjestelmä Moodle tukee ipv6-protokollaa versiosta 2.0 lähtien (Moodle 2010). Moodlen päivittäminen uudempaan versioon edellyttää, että Moodlen käyttämät muut ohjelmistot, Apache, MySQL ja PHP, tukevat myös ipv6-protokollaa (Moodle 2012). MySQL:n ipv6-tuki alkaa versiosta 6 (MySQL 2012).

CIFS / DFS

Windows Server 2003:lla ja Server 2008:lla toteutettu Cifs-tiedostonjakopalvelin tukee ipv6-protokollaa. Windows Vistassa ja 7:ssa on sisäänrakennettu, ipv6-protokollaa käyttävä CIFS-asiakasominaisuus. (Morr 2009.) Samba:lla toteutettavassa tiedostonjaossa on käytettävä vähintään versiota 3.2, josta lähtien ipv6-protokolla on tuettu (Samba 2008).

SCCM

Microsoftin System Center Configuration Manager 2007 tukee ipv6-protokollaa (Microsoft 2012).

Remote Desktop

Remote desktop -toiminto testattiin kahdella virtuaalitietokoneella, jotka olivat samassa aliverkossa. Virtuaalipalvelimessa sallittiin etähallinta sekä palomuurissa sallittiin etähallintayhteys. Virtuaalisella asiakaskoneella muodostettiin yhteys virtuaalipalvelimeen ja sisäänkirjautumisen jälkeen virtuaalipalvelinta päästiin hallitsemaan virtuaalisen asiakaskoneen avulla. Etähallinta ipv6-protokollalla toimi täsmälleen samalla lailla kuin ipv4:llakin. Virallista tietoa etähallinnan toimivuudesta ipv6-protokollalla ei löytynyt Microsoftin sivuilta.

5 IPV6-TESTIYMPÄRISTÖN RAKENTAMINEN JA TESTAAMINEN

5.1 Rakentaminen

Ipv6-testiympäristön rakentaminen aloitetaan palvelimen rakentamisesta. Tässä tapauksessa palvelimena käytetään kannettavaa tietokonetta, johon asennettaan Windows Server 2008 R2 SP1 kaikilla päivityksillä. Palvelimen Hyper-V -– ominaisuutta hyödynnetään asentamalla palvelimeen uusi Windows Server 2008 R2 SP1 kaikilla päivityksillä virtuaalisesti. Aluksi virtuaalisen Windows Server 2008 R2-palvelimen asennus- ja päivitystoimenpiteitä varten virtuaalipalvelimelle annetaan resursseina molemmat prosessorin ytimet sekä 1,2 GB keskusmuistia. Raskaiden asennus- ja päivitystöiden jälkeen resursseja vähennetään niin, että virtuaalipalvelimelle annetaan yksi prosessori ja keskusmuistia 512 MB. Alkuperäinen virtuaalinen palvelin kloonataan kahdeksi virtuaalipalvelimeksi eri palveluita varten ja virtuaalipalvelimille annetaan nimet WS1 ja WS2. Lisäksi palvelimelle asennetaan virtuaaliseksi asiakaskoneeksi Windows 7 Enterprise, joka päivitetään ajan tasalle ja nimetään Oppilas-PC:ksi.

Virtuaalipalvelimissa ja asiakaskoneessa käytetään sisäänrakennettua palomuuria, jotta säästetään keskusmuistia. Virtuaalipalvelimiin tehdään palomuuriin sääntö, jolla sallitaan ICMPv4- ja ICMPv6-liikenne. Säännöt tehdään, koska työn testaamisessa tullaan tarvitsemaan ping- ja nslookup-toimintoja.

WS1-virtuaalipalvelimesta tehdään Domain Controller -palvelin (DC) asentamalla DC-palvelu rooliksi virtuaalipalvelimeen. DC-roolia asentaessa täytyy samaan palvelimeen asentaa myös DNS-palvelin, joka asennetaan ja domain-nimeksi annetaan v6.lpt.fi. Samassa verkossa on myös unix-pohjainen DNS-palvelin, joka pyytää nimitiedot juuripalvelimilta. Tämän unix-pohjaisen DNS-palvelimen domain on ipv6.lpt.fi.

Kun DC-rooli saadaan asennettua, muutetaan WS1-virtuaalikoneen ip-osoitteet. Ipv4-osoiteeksi annetaan 192.168.31.99 maskilla 24, oletusyhdyskäytäväksi 192.168.31.1 ja DNS-palvelimeksi oma ip-osoite. Ipv6-osoitteiksi annetaan 2001:708:410:778::99, maskiksi /64, oletusyhdyskäytäväksi 2001:708:410:778::1 ja DNS-palvelimeksi oma ipv6-osoite.

DC-palvelimelle luodaan ryhmä Kayttajat ja sinne käyttäjä paularid. Tämä tehdään Server Manager -ikkunassa Active Directory:n alla klikkaamalla hiiren oikealla ja valitsemalla New ja Group. Kun ryhmä on luotu, luodaan käyttäjä paularid ryhmään Kayttajat klikkaamalla hiiten oikealla kohtaa Kayttajat, valitsemalla New ja User. Käyttäjälle annetaan nimi, kirjautumistunnus ja salasana. Edetään loppuun saakka ja uutta käyttäjätunnusta voidaan kokeilla Oppilas-pc:llä.

WS2-virtuaalipalvelimen rooli on toimia verkkojakopalvelimena, jossa sijaitsee eri käyttäjätunnusten verkkotallennustilat. Ennen roolin asentamista WS2-virtuaalipalvelimelle annetaan kiinteät ip-osoitteet. Ipv4-osoitteet ovat 192.168.31.98 maskilla 24, oletusyhdyskäytäväksi 192.168.31.1 ja DNS-palvelimeksi 192.168.31.99. Ipv6-osoitteiksi annetaan 2001:708:410:778::98, maskiksi /64, oletusyhdyskäytäväksi 2001:708:410:778::1 ja DNS-palvelimeksi 2001:708:410:778::99. Osoitteiden antamisen jälkeen WS2-virtuaalipalvelin liitetään v6-domain -verkkoon.

Rooli asennetaan normaalisti ja levyjaon käyttöönotossa käytetään velhoa, jossa nimeksi annetaan WS2_jako ja jatketaan eteenpäin. Seuraavaksi valitaan jaon tyyppi, johon valitaan Domain-perusteinen jako. Seuraavaksi käydään luomassa velhon ilmoittamaan kansioon jaettava kansio. Kansiolle annetaan nimeksi Kayttajat.

DC-palvelimen polkuun c:\windows\sysvol\sysvol\testi.local\scripts luodaan cmd-päätteinen tiedosto mounttaus.cmd, jonka sisältönä on net use y: \\WS2\Kayttajat$\%username%. DC-palvelimen käyttäjien ominaisuuksista määritellään skripti ajettavaksi logon-vaiheessa. Käyttäjän kirjautuessa tietokoneelle skripti yhdistää käyttäjän omaan kotikansioonsa. Levynjakoa kokeillaan Oppilas-pc:llä kirjautumalla paularid-tunnuksella Oppilas-pc:lle ja sisäänkirjautumisen jälkeen katsotaan näkyykö jakokansiota Resurssienhallinnasta ja se näkyy. Tiedostonjakoa kokeillaan lataamalla Oppilas-pc:llä internetistä Mozilla Firefoxin asennuspaketti ja siirtämällä paketti verkkolevylle. WS2-palvelimelta katsotaan Kayttajat-kansioon ja siellä sijaitsee Mozilla Firefoxin asennuspaketti. Verkkojako toimii.

5.2 Testaussuunnitelma

Työssä luotiin testaussuunnitelma, jonka mukaan testejä aletaan suorittaa testiympäristössä, kun testiympäristö saadaan valmiiksi. Operaattorin viivästyksen vuoksi käytännön testaamista ei voitu suorittaa ajallaan tähän opinnäytetyöhön. Testaukset suoritetaan erikseen opinnäytetyön ulkopuolella. Taulukossa viisi on havainnollistettu yksinkertainen testausjärjestys. Testiympäristössä on tarkoitus testata ohjelmistojen ja palveluiden toiminta molemmilla protokollilla tuotantoverkkoa vastaavassa testiverkossa. Jotkin ohjelmistot ovat hankalia testata ennakkoon testiympäristössä esimerkiksi lisenssien takia, joten niitä voidaan testata tuotantoverkossa dual stack -siirtymätekniikan ansiosta. Ipv6-protokollan kanssa yhteensopimaton ohjelmisto pitäisi toimia normaalisti, vaikka verkossa kulkisikin myös ipv6-liikennettä.

Kaikkien ohjelmistojen ipv6-tukea ei löydy ohjelmiston valmistajan sivustoilta eikä tukikeskustelusivustoilta. Näiden ohjelmistojen ipv6-tuki selviää parhaiten testaamalla suoraan palvelin-asiakas -testillä. Molempiin laitteisiin määritellään ipv4- ja ipv6 -osoitteet ja testataan toimiiko ohjelmisto. Tämän jälkeen voidaan ipv4-osoitteet poistaa käytöstä ja kokeilla, toimiiko ohjelmisto edelleen. Jos ipv6-protokollalla ohjelmisto ei toimi, ohjelmiston mahdollista päivittämistä kannattaa harkita tai jatkaa sen käyttöä vielä ipv4-protokollalla, koska siirtymäaika tulee olemaan pitkä.

PHKK:n tapauksessa ulkopuoliselta ohjelmointiyritykseltä tilattu Winha-järjestelmä on epävarma sovellus. Winhan koodia ja rakennetta ei päästy tutkimaan tämän työn yhteydessä. Winhan iästä voisi päätellä, että sovelluksen nykyinen versio on vanhentunut ja saaneen päivityksen lähiaikoina.

Tiedostonjakoa testattiin kahdella virtuaalikoneella samassa aliverkossa ja tiedostonjako toimi hyvin. Tiedostonjakoa pitää vielä testata eri aliverkkojen välillä siten, että tiedostopalvelin ja asiakaskone sijaitsevat eri aliverkoissa. Linux-pohjaista tiedostonjakoa voidaan testata samalla tavalla.

Microsoft Exchange -sähköpostipalvelu pitää rakentaa vähintään Windows Server 2008 -version päälle, jotta ipv6-protokollaa voidaan käyttää. Exchangen kaikki

komponentit eivät vielä tue ipv6-protokollaa. Tukemattomat komponentit löytyvät listattuna Microsoftin sivuilta. Testaamistyössä testataan Exchangen tärkeimpien komponenttien toiminta ipv6-protokollalla.

SCCM:n ja remote desktopin testaaminen tehdään samoin kuin tiedostonjaonkin, testataan eri aliverkoista toiseen. Virallista tietoa remote dekstopin toiminnasta ipv6-protokollalla ei ole, mutta käytännön pieni testi on osoittanut, että remote desktop toimii ipv6:lla samoin kuin ipv4:lla.

TAULUKKO 5. Yksinkertaiset testaukset

Testattava asia	Testausmenetelmä
Käyttöjärjestelmän ipv6- ja dual stack -tuki.	Yritetään antaa käyttöjärjestelmään ipv6-osoite yhtäaikaa ipv4-osoitteen kanssa.
Ping	Osoitteen antamisen jälkeen kokeillaan pingata oletusyhdyskäytävää tai julkista ipv6-osoitetta.
DHCPv6:n toimivuus	Poistetaan ipv6-osoite ja kokeillaan, saako tietokone ipv6-osoitteen DHCPv6-palvelimelta
Ping	Osoitteen saatuaan kokeillaan pingata oletusyhdyskäytävää tai julkista ipv6-osoitetta.
Tiedostonjako eri ipv6-aliverkoista	Testataan, toimiiko tiedostonsiirto eri aliverkosta olevalta koneelta palvelimelle.
Etähallinta eri ipv6-aliverkoissa.	Kaksi tietokonetta kytketään eri aliverkkoon ja kokeillaan muodostaa etähallintayhteys ipv6:lla.

Taulukossa kuusi on esitetty testattavat asiat, jotka ovat suurempitöisiä ja vaativat enemmän rakentelua. Taulukossa kuusi lueteltujen ohjelmistojen pitäisi ohjelmistovalmistajien mukaan tukea ipv6-protokollaa. PHP, IIS ja Exchange eivät vielä tue täydellisesti ipv6-protokollaa. Microsoftin mukaan SCCM tukee

ipv6-protokollaa, mutta SCCM:n toiminnan voi testata, jos sen kokee tarpeelliseksi.

TAULUKKO 6. Monimutkaisemmat testaukset

Testattava asia	Testausmenetelmä
Microsoft IIS	Rakennetaan testisivusto IIS:llä ja kokeillaan sen toimivuuta.
LAMP-paketti	Testataan Linux, Apache, MySQL ja PHP:n ipv6-toimivuus rakentamalla testisivusto.
Moodle	Järjestelmä rakentuu LAMP:ssa. Asennetaan moodle, apuohjelmat ja testataan toiminta.
Exchange	Testataan Exchangen eri komponenttien ipv6-toiminta.
SCCM	Valmistajan mukaan tukee, tämän voi kyllä testata.

6 YHTEENVETO

Tämä opinnäytetyön aiheena käsitellään ja tutkitaan ipv6-protokollaa ja siihen siirtymistä sekä eri ohjelmistojen ja palveluiden toimintaa ipv6-protokollan kanssa. Ipv4-protokollan osoitteet ja ominaisuudet eivät enään riitä nykypäivän internetin käyttöön ja käyttäjämäärille. Siirtyminen ipv6-protokollaan on aloitettava hiljalleen, jotta uusi protokolla saataisiin käyttöön ja vanhan käyttäminen loppuisi.

Työn tavoitteena oli tutustua ipv6-protokollaan, sen ominaisuuksiin, eri siirtymistekniikoihin ja eroaisuuksiin ipv4-protokollaan nähden sekä tutkia, miten PHKK:n ohjelmistot ja palvelut tukevat ipv6-protokollaa ja mitä päivityksiä pitäisi tehdä. Testiympäristössä oli tarkoitus kokeilla eri ohjelmistojen toimintaa käyttäen ipv6-protokollaa, mutta testiympäristön verkko ei valmistunut ajoissa. Testiympäristön verkko tarvitsi tuotantoverkon laitteita toimiakseen, mutta niiden ohjelmistoversiot eivät tukeneet ipv6-protokollaa.

Prokollien eroavaisuudet ovat aika selkeitä. Ipv6-protokollan erilainen kehysrakenne, osoitteistus ja osoitteiden rakenne ovat merkittävimmät erot. Kehysrakenne on joustavempi tarjoten paremman muokattavuuden erilaisille sovelluksille. Osoitteistus poikkeaa pituudeltaan ipv4-protokollan osoitteisiin nähden ja osoiteavaruuden koko on huomattavasti suurempi kuin vanhassa protokollassa. Osoitteiden rakenne hieman hankaloittaa osoitteiden laskemista. Aliverkkojen käyttö on tehty yksinkertaisemmaksi sisällyttämällä aliverkon tunnus ipv6-osoitteeseen. Osoitteiden määrän lisäksi uudenlainen osoitteistus mahdollistaa osoitteiden fiksumman ja loogisemman käytön sekä jakamisen, mikä helpottaa reititysprosesseja.

Työssä saatiin selvitettyä eri käyttöjärjestelmien ja eri palveluiden tuki ipv6-protokollalle. Palveluista osa odottaa vielä päivityksiä ja tukea ipv6-protokollalle, mutta suurimmassa osassa palveluita tuki on. Microsoft Exchangen ja SCCM:n tapauksessa luotetaan valmistajan tietoon ipv6-protokollan tukemisesta.

Siirtymävaiheessa dual stack -tekniikan käyttäminen on hyvä ratkaisu. Dual stackilla varmistetaan, että jokainen asiakas saa muodostettua yhteyden

haluamaansa palveluun joko ipv4- tai ipv6 -protokollaa hyväksikäyttäen. Dual stack -tekniikka helpottaa siirtymävaiheen työtä, koska molemmat protokollat ovat yhtäaikaa käytössä ja kun on aika siirtyä lopullisesti ipv6-protokollaan, poistetaan kaikki ipv4-protokollaan liittyvä.

Kun operaattori on saanut päivitettyä PHKK:n reitittimet ja palomuurit, voidaan työtä jatkaa testaussuunnitelman mukaan. Operaattorin päivitykset ja testiympäristön testaaminen eivät aivan ehtineet tähän opinnäytetyöhön, joten ne tehdään, kun kaikki päivitykset ovat valmiita. Testaussuunnitelmassa testit jaoteltiin yksinkertaisiin ja monimutkaisiin testeihin. Yksinkertaiset testit pystytään testaamaan nykyisellä testiympäristöllä, mutta monimutkaiset testit vaativat suurempaa rakentamista, sillä kyseiset testauskohteet ovat omia järjestelmiä.

PHKK:n siirtyminen ipv6-protokollaan tapahtunee parin, kolmen vuoden sisällä, kun kaikki PHKK:n käyttämät järjestelmät ja tarjoamat palvelut tukevat ipv6-protokollaa täydellisesti. PHKK:n tuottamia palveluita ja palvelimia käytetään laajasti ja käyttäjiä on paljon, joten siirtymisprosessi on hoidettava nopeasti ja kaikki on saatava toimimaan. Paras ajankohta päivitykselle lienee kesällä, jolloin käytön pitäisi olla vähäisintä.

Yrityksien siirtyminen ipv6-protokollaan riippuu paljon operaattoreiden tarjoamasta palvelusta, sen hinnoittelusta, siirtymisen kustannuksista ja laitehankinnoista. Jos yrityksen täytyy uusia isompi osa laitteistoaan nykyaikaiseksi, yritys voisi siirtyä käyttämään ipv6-protokollaa dual stack -tekniikalla. Operaattoreiden aktiivisuus ja halukkuus siirtää asiakkaita käyttämään ipv6-protokollaa vaikuttanee yrityksien päätöksentekoon siirtymisestä.

Maailmanlaajuisesti siirtyminen ipv6-protokollaan alkanee parin, kolmen vuoden sisällä, kunhan ensin nykyiset ipv4-osoitteet loppuvat. Siirtymäaika lienee kymmenen vuoden luokkaa, koska kaikkialla maailmassa ei ole käytössä uusimpia laitteita eivätkä kaikki operaattorit ja yritykset ole valmiita sijoittamaan päivitykseen. Siirtymäajan jälkeenkin ipv4-protokolla saattaa olla käytössä vanhoissa sisäverkoissa ja palveluissa, joita ei voida tai ei kannata päivittää tukemaan ipv6-protokollaa. Muutaman vuoden päästä siirtymän alettua on tarvetta

ipv6-protokollan osaaville työntekijöille. Ipv6-protokollan osuutta ja opetusta pitäisi lisätä toisen- ja korkeakouluasteen koulutuksessa.

LÄHTEET

Aben, E. 2010. 6to4 - How Bad is it Really? [viitattu 16.2.2012]. Saatavissa: https://labs.ripe.net/Members/emileaben/6to4-how-bad-is-it-really

Aben, E. 2011. 6to4 - Why is it so Bad? [viitattu 16.2.2012]. Saatavissa: https://labs.ripe.net/Members/emileaben/6to4-why-is-it-so-bad

Bieringer, P. 2009. Linux Ipv6 Howto [viitattu 14.2.2012]. Saatavissa: http://tldp.org/HOWTO/Linux+IPv6-HOWTO/systemcheck-kernel.html

Cisco, Comcast, Durand, A., Ward, D., Wing, D. 2008. A Comparison of Proposals to Replace NAT-PT draft-wing-nat-pt-replacement-comparison-02 [viitattu 16.2.2012]. Saatavissa: http://www.viagenie.ca/ietf/draft/draft-wing-nat-pt-replacement-comparison-02.txt

Cisco. 2011a. DHCPv6 Based IPv6 Access Services [viitattu 2.2.2012]. Saatavissa: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553/whitepaper_c11-689821.html

Cisco. 2011b. How NAT Works [viitattu 31.1.2012]. Saatavissa: http://www.cisco.com/en/US/tech/tk648/tk361/technologies_tech_note09186a0080094831.shtml

Cisco. 2012. Ipv6 Routing At A Glance [viitattu 2.2.2012]. Saatavissa: www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80260051.pdf

Comer, D. E. 2002. TCP/IP. Jyväskylä: Gummerus.

Davies, J. 2008. IPv6 Transition Technologies [Viitattu 6.2.2012]. Saatavissa: http://technet.microsoft.com/fi-fi/library/bb726951%28en-us%29.aspx

Desmeules, R. 2007. Cisco Self-Study. Indianapolis, USA: Cisco Press.

Ecdysis. 2012. Why Translate between IPv4 and IPv6? [viitattu 16.2.2012]. Saatavissa: http://ecdysis.viagenie.ca/whynat64.html

Google. 2011. Google over IPv6 [viitattu 14.2.2012]. Saatavissa: http://www.google.com/intl/en/ipv6/

IBM. 2012. Comparison of Ipv4 and Ipv6 [viitattu 2.2.2012]. Saatavissa: http://publib.boulder.ibm.com/infocenter/iseries/v5r4/index.jsp?topic=%2Frzai2%2Frzai2compipv4ipv6.htm

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo.

Kaushik, D. 2012. What is Mobile Ipv6? [viitattu 6.2.2012]. Saatavissa: http://ipv6.com/articles/mobile/Mobile-IPv6.htm

Kerr, S. 2006. DHCPv6 [viitattu 2.2.2012]. Saatavissa: meetings.ripe.net/ripe-53/presentations/dhcpv6.pdf

Kline, E. 2012. Ipv6: countdown to launch [viitattu 14.2.2012]. Saatavissa: http://googleblog.blogspot.com/2012/01/ipv6-countdown-to-launch.html

Linux. 2011. Ipv6-tunneli [viitattu 16.2.2012]. Saatavissa: http://linux.fi/wiki/IPv6-tunneli

Livinginternet. 2012. Internet history – One page summary [viitattu 17.1.2012]. Saatavissa: http://www.livinginternet.com/i/ii_summary.htm

Marsan C.D 2010. Facebook adds Ipv6 support [viitattu 14.2.2012]. Saatavissa: http://www.networkworld.com/news/2010/061110-facebook-ipv6.html

Microsoft Technet. 2011a. IPv6 Support in Exchange 2007 SP1 and SP2 [viitattu 21.2.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/bb629624%28v=exchg.80%29.aspx

Microsoft TechNet. 2011b. Understanding IPv6 Support in Exchange 2010 [viitattu 21.2.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/gg144561.aspx

Microsoft TechNet. 2012. How IIS 6.0 Supports IPv6 (IIS 6.0) [viitattu 21.2.2012]. Saatavissa:

http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/1ecff3af-36c2-41b5-957a-8bcc6fac8abc.mspx?mfr=true

Microsoft. 2012. Configuring DNS for Configuration Manager Site System Roles [viitattu 23.2.2012]. Saatavissa: http://technet.microsoft.com/en-us/library/bb632341.aspx

Moodle. 2010. Full Ipv6 support (MDL-14123) [viitattu 21.2.2012]. Saatavissa: http://tracker.moodle.org/browse/MDL-14123?page=com.atlassian.jira.plugin.system.issuetabpanels:all-tabpanel#issue-tabs

Moodle. 2012. Complete install packages for Windows [viitattu 21.2.2012]. Saatavissa: http://docs.moodle.org/22/en/Complete_install_packages_for_Windows

Morimoto, R. 2011. Configuring Microsoft Active Directory to Support IPv6 [viitattu 16.2.2012]. Saatavissa: http://www.networkworld.com/community/blog/configuring-microsoft-active-directory-suppor

Morr, D. 2009. Ipv6 on Windows [viitattu 23.2.2012]. Saatavissa: https://wikispaces.psu.edu/display/ipv6/IPv6+on+Windows

MySQL. 2012. MySQL On ipv6 [viitattu 13.4.2012]. Saatavissa: http://lists.mysql.com/mysql/219540

Opasmedia. 2012. Ensiaskeleet [viitattu 17.1.2012]. Saatavissa: http://www.internetopas.com/historia/

Päijät-Hämeen koulutuskonserni. 2012a. Esittely [viitattu 13.4.2012]. Saatavissa: http://www.phkk.fi/esittely/

Päijät-Hämeen koulutuskonserni. 2012b. Tietohallintopalvelut, toiminnot ja tehtävät [viitattu 15.4.2012]. Saatavissa: http://www.phkk.fi/yhteisetpalvelut/thy/toiminnot.html

RFC 1349. 1992. Type of Service in the Internet Protocol Suite [viitattu 30.1.2012]. Saatavissa: http://www.ietf.org/rfc/rfc1349.txt

RFC 2450. 1998. Proposed TLA and NLA Assignment Rules [viitattu 30.1.2012]. Saatavissa: http://www.ietf.org/rfc/rfc2450.txt

RFC 2474. 1998. Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers [viitattu 30.1.2012]. Saatavissa: http://tools.ietf.org/html/rfc2474

RFC 2893. 2000. Transition Mechanisms for IPv6 Hosts and Routers [viitattu 30.1.2012]. Saatavissa: https://tools.ietf.org/html/rfc2893

RFC 3053. 2001. IPV6 Tunnel Broker [viitattu 9.2.2012]. Saatavissa: http://tools.ietf.org/html/rfc3053

RFC 4213. 2005. Basic Transition Mechanisms for IPv6 Hosts and Routers [viitattu 30.1.2012]. Saatavissa: https://tools.ietf.org/html/rfc4213

RFC 4291. 2006. IP Version 6 Addressing Architecture [viitattu 30.1.2012]. Saatavissa ftp://ftp.ripe.net/rfc/rfc4291.txt

Rinta, N. 2012. Ip-osoitteet loppuvat Euroopasta heinäkuussa 2012. Talentum. [viitattu 26.1.2012]. Saatavissa: http://www.tietoviikko.fi/kaikki_uutiset/iposoitteet+loppuvat+euroopasta+heinakuussa+2012/a749382

Samba.org. 2008. Samba Team Releases Samba 3.2 [viitattu 23.2.2012]. Saatavissa: http://news.samba.org/announcements/3.2_press_release/

Sellers, C. 2009. Ipv6 Transition Mechanisms and Strategies [viitattu 24.4.2012]. Saatavissa: http://www.rmv6tf.org/2009-IPv6-Summit-Presentations/Chuck%20Sellers%20-%20090421-IPv6-Transition-Mechanisms-Sellers.pdf

Sourcedaddy. 2012. Ipv6 support [viitattu 7.2.2012]. Saatavissa: http://sourcedaddy.com/windows-7/ipv6-support.html

The Apache Software Foundation. 2012. Overview of new features in Apache 2.0 [viitattu 21.2.2012]. Saatavissa: http://httpd.apache.org/docs/2.2/new_features_2_0.html

The Ipv6 Portal. 2012. Using ipv6 – connectivity [viitattu 16.2.2012]. Saatavissa: http://www.ipv6tf.org/index.php?page=using/connectivity/6to4

The TCP/IP Guide. 2005. DHCP For IP Version 6 (DHCPv6) [viitattu 2.2.2012]. Saatavissa: http://www.tcpipguide.com/free/t_DHCPForIPVersion6DHCPv6-2.htm

Tuminauskas, R. 2011. Experimental NAT64/DNS64 Service [viitattu 16.2.2012]. Saatavissa: https://labs.ripe.net/Members/raimis/experimental-nat64-dns64-service

Wikipedia. 2012a. OSI model [viitattu 16.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/OSI_model

Wikipedia. 2012b. Session layer [viitattu 16.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/Session_layer

Wikipedia. 2012c. TCP/IP-viitemalli [viitattu 17.1.2012]. Saatavissa: http://fi.wikipedia.org/wiki/TCP/IP-viitemalli

Wikipedia. 2012d. TCP/IP model [viitattu 17.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/TCP/IP_model#cite_ref-Comer_12-0

Wikipedia. 2012e. Internet [viitattu 17.1.2012]. Saatavissa: http://fi.wikipedia.org/wiki/Internet

Wikipedia. 2012f. History of the Internet [viitattu 17.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/History_of_the_Internet

Wikipedia. 2012g. Classless Inter-Domain Routing [viitattu 19.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/Classless_Inter-Domain_Routing

Wikipedia. 2012h. Osoitteenmuunnos [viitattu 19.1.2012] Saatavissa: http://fi.wikipedia.org/wiki/Osoitteenmuunnos

Wikipedia. 2012i. IP address [viitattu 19.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/IP_address

Wikipedia. 2012j: Ipv4 Addressing [viitattu 19.1.2012]. Saatavissa: http://en.wikipedia.org/wiki/IPv4#Addressing

Windows-ipv6. 2011. Windows IPv6 Implementation [viitattu 7.2.2012]. Saatavissa: http://www.windows-ipv6.org/index.php?page=implementation

Wmware. 2011. Configuring Ipv6 on ESX 4.0.x [viitattu 20.2.2012]. Saatavissa: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1010812